

# Personvern i elektroniske billettsystemer

Avdeling for forvaltningsinformatikk  
Juridisk fakultet  
Universitetet i Oslo

Erling Rostvåg  
01.09.2012

## Forord

Denne oppgaven, eller i det minste en versjon av den, ble først påtenkt høsten 2010. Siden den gang har oppgaven sakte, men sikkert utviklet fasongen og strukturen den har i dag.

Arbeidet har vært knallhardt, og jeg har vært helt avhengig av støtte fra kolleger, venner og studiekamerater. Takk til Silje Eckermann Falck for tålmodigheten. Takk til Marit Torseth, min evige sparringspartner og kompanjong på kontoret for innspill og hjernestorming. Takk til Gisle Rostvåg for korrekturlesing og språklig støtte.

Takk til et flott miljø på SERI/AFIN for at dere besitter den uslåelige kombinasjonen av å være trivelig og faglig sterke. Spesiell takk til Dag Wiese Schartum og Thom-Kåre Granli for juridiske råd og vink og ikke minst takk til Tommy Tranvik for veiledning og tålmodighet fra start til slutt.

## Innhold

1.0 Elektroniske billettsystemer og personvern .....	6
1.1 Introduksjon til temaet .....	6
1.2 Nærmere om problemstillingen .....	7
1.3 Personvernperspektiver .....	8
1.3.1 Beslutningsperspektivet på personvern .....	8
1.3.2 Integritetsperspektivet på personvern .....	9
1.3.3 Maktperspektivet på personvern .....	10
1.3.4 Personvernperspektivene i forhold til elektroniske billettsystemer .....	11
1.3.5 Interesseteorien .....	12
1.3.6 Personopplysning eller ikke? .....	13
1.4 Utvalg av caser .....	13
1.5 Konkret om casene .....	14
1.5.1 Bakgrunnen for Innlandskortet .....	14
1.5.2 Bakgrunnen for Reisekortet .....	15
1.6 Kapitteloversikt .....	16
2.0 Metode .....	17
2.1 Arbeidsmetodikk .....	18
2.2 Juridisk metode .....	18
2.3 Intervjuene .....	19
2.4 Dokumentstudier .....	20
2.5 Nettkilder .....	21
2.6 Begrensninger og svakheter ved metoden .....	21
2.6.1 Hovedutfordringen underveis .....	22
3. 0 Juridiske drøftelser .....	23
3.1 Sentrale bestemmelser i personopplysningsloven .....	23
3.2 Å knytte en opplysning til en person .....	26
3.2.1 Opplysninger knyttet til uregistrerte kort .....	27
3.2.2 Kortets tilknytning til den registrerte .....	29
3.2.3 Scenario 1 .....	31
3.2.4 Scenario 2 .....	32
3.2.5 Drøftelse .....	33
3.2.6 Konklusjon .....	35

3.3 Samtykket har prioritet .....	36
3.3.1 Foreløpig oppsummering om samtykke.....	38
3.4 Nødvendighetsgrunnene.....	38
3.4.1 Formålet med behandlingen .....	39
3.4.2 Formålene som ikke krever behandling av personopplysninger .....	42
3.4.3 Formålene som krever behandling av personopplysninger .....	43
3.4.4 Billettkontroll .....	47
3.4.5 Skoleskyssordningen.....	47
3.5 Rettslige krav til samtykke.....	48
3.5.1 "Frivillig" .....	50
3.5.2 "Informert" .....	51
3.5.3 "Utrykkelig" .....	52
3.6 Krav til gjennomføring av samtykke i praksis .....	53
3.6.1 Nærmere om den foreløpige kravlisten .....	54
3.6.2 Oppsummering .....	59
3.7 Uforholdsmessig vanskelig å innhente samtykke? .....	60
4.0 Dagens praksis hos Reisekortet .....	60
4.1 Generelt om informasjon som gis på nettsiden .....	61
4.2 Registreringsprosessen på nett .....	66
4.3 Andre kilder til informasjon .....	70
4.4 Drøftelse av Reisekortets praksis.....	70
4.5 Oppsummering av reisekortets praksis .....	76
5.0 Dagens praksis hos innlandskortet.....	78
5.1 Generelt om informasjon som gis på nettsidene .....	78
5.2 Registreringsprosessen på nett .....	81
5.3 Andre kilder til informasjon .....	82
5.4 Drøftelse av innlandskortets praksis .....	82
5.5 Oppsummering.....	86
6.0 Bransjenormen .....	87
6.1 Generelt om Bransjenormen .....	88
6.2 Samtykke og frivillighet i Bransjenormen .....	89
6.3 Innsyn, sletting og retting i Bransjenormen .....	90
6.4 Øvrige bestemmelser i Bransjenormen .....	91

6.5 Oppsummering av Bransjenormen.....	92
6.6 Reisekortet og Innlandskortet i lys av Bransjenormen. ....	93
7.0 Oppsummering og samlede vurderinger.....	95
7.1 Problemstillingen oppsummert.....	95
7.2 utfordringer i bransjen.....	96
7.2.1 Lovtolkning .....	96
7.2.2 Utvikling av billettsystemene .....	97
7.3 Bransjenormen og veien videre .....	97
Kilder: .....	99
Litteratur:.....	99
Rettskilder: .....	100
Internettkilder: .....	101

## 1.0 Elektroniske billettsystemer og personvern

I denne oppgaven skal jeg se nærmere på hva slags informasjon om brukeren som samles inn når elektroniske billetter benyttes i kollektivtrafikken. Jeg skal undersøke hvor mye av dette som er personopplysninger, hvilke behandlingsgrunnlagsom er tilgjengelige for å behandle disse opplysningene, og hvilke krav som stilles for at behandlingen skal være lovlig utført.

Oppgaven vil bruke Ruters Reisekortet og Innlandskortet, et samarbeid mellom Hedmark trafikk og Oppland trafikk, som eksempler og kilder for nærmere undersøkelser av hva praksis er i dag.

### 1.1 Introduksjon til temaet

Elektroniske billettsystemer blir stadig vanligere å benytte seg av. Mest kjent er kanskje det mye omtalte Flexus som etter store forsinkelser, mange medieoppslag og en navneendring nå er tatt i bruk og tilgjengelig for i overkant av 1,4 millioner mennesker.<sup>1</sup> Det som kanskje ikke har kommet like tydelig fram i mediebildet er at elektroniske billettsystemer tas i bruk over hele landet og at flere av dem har vært i bruk i lang tid.<sup>2</sup>

Det er åpenbart gode grunner til å ta i bruk elektroniske billettsystemer mange steder i landet. Det er sannsynligvis store penger å spare på å strømlinjeforme selvbetjeningsløsningene og det kan øke tilgjengeligheten om tilbudet kan administreres av den enkelte bruker hjemmefra. Kollektivtransportprodusentene kan også få verdifull innsikt i sine brukeres reisevaner<sup>3</sup> og det kan til og med være en liten miljøgevinst i å erstatte papirbillettene.

Dette er trolig årsak til at bruken av elektroniske billettsystemer øker i omfang og at stadig flere administrasjonsselskaper, kommuner og fylkeskommuner allerede har erstattet eller planlegger å erstatte papirbillettene helt.<sup>4</sup>

Samtidig skaper dette nye utfordringer som papirbillettene ikke bød på. Jeg skal se nærmere på opplysningene som samles inn ved bruk av elektroniske billettsystemer og de personvernutfordringer dette bringer med seg. Elektronisk behandling av personopplysninger reguleres i personopplysningsloven (heretter popplyl) og

---

<sup>1</sup> Folketallet i Stor-Osloregionen befant seg et sted mellom 1,4 og 1,5 millioner i 2011 i følge SSB. *Befolkningsendringer 2010 - 2011*, URL: <http://www.ssb.no/folkendrkv/arkiv/tab-2011-02-24-02.html>

<sup>2</sup> Kolumbuskortet i Rogaland ble tatt i bruk i 2006, Tromskortet i 2006, Skysskortet i Hordaland i 2008 og Innlandskortet i Hedmark og Oppland i 2007 for å nevne noen. Sistnevnte hadde også elektroniske billetter i to separate systemer før de slo seg sammen.

<sup>3</sup> OsloTrikken har for eksempel erfaringer med at "Rullende Fortau" – en endring i kjøremønster som garanterer at en trikk passerer til faste korte intervaller, førte til reduserte kostnader og flere passasjerer: OsloTrikken (2007), side 4, URL: [http://www.trikken.no/OpplastedeBilder/DivBilde/OSSP0026\\_Aarsrapport.pdf](http://www.trikken.no/OpplastedeBilder/DivBilde/OSSP0026_Aarsrapport.pdf)

<sup>4</sup> For eksempel Wikipedia: "Flexus", 2. avsnitt, URL: <http://no.wikipedia.org/wiki/Flexus> og Sør-Trøndelag Fylkeskommune (2003), side 2, URL: <http://www.revisjonmidtnorge.no/rapporter/2003-elektroniskbillettering.pdf>

personopplysningsforskriften (heretter pof) og jeg vil derfor se nærmere på forholdet mellom billettsystemene og lovverket.

I denne oppgaven skal jeg svare på følgende spørsmål om bruken av elektroniske billetter i kollektivtrafikken:

- 1) Hva brukes som behandlingsgrunnlag for opplysningene som samles inn?
- 2) Hvilke rettslige krav stilles til behandlingsgrunnlaget selskapene benytter seg av?
- 3) Hvordan er praksis for innsamling av personopplysninger og informasjon til de registrerte i selskapene?
- 4) I hvilken grad er praksis hos selskapene i tråd med de rettslige krav som stilles etter spørsmål 2?

Dette er med andre ord en todelt problemstilling der jeg først vil utrede hvilke rettslige krav som gjelder for behandling av personopplysninger i elektroniske billettsystemer med særlig fokus på behandlingsgrunnlag. Deretter vil jeg se på selskapenes praksis med særlig fokus på graden av regeletterlevelse.

Denne drøftelsen krever at jeg forsøker å kartlegge gjeldende rett på området. Videre vil jeg velge to caser som representanter for dagens praksis og sammenligne funnene i den juridiske kartleggingen med undersøkelser hos casene. Jeg ønsker å se på i hvilken grad dagens praksis harmonerer med rettslige krav. Disse fire spørsmålene reiser også en del underspørsmål som jeg skal gå gjennom i neste kapittel.

## 1.2 Nærmere om problemstillingen

Begge casene mine er veldig tydelige på at behandlingsgrunnlaget de benytter seg av er samtykke (spørsmål 1). Det finnes unntak gjennom skoleskyssordningen<sup>5</sup> og i forbindelse med billettkontroll, men disse er unntaket heller enn regelen og noe jeg skal se nærmere på henholdsvis i kapittel 3.4.5 og 3.4.4.

For at samtykke som behandlingsgrunnlag skal kunne tas i bruk stilles det en rekke rettslige krav, både prosessuelle og materielle krav.<sup>6</sup> Disse blir jeg nødt til å utrede nærmere (spørsmål 2). Ettersom to caser ikke kan sies å være et representativt utvalg vil jeg i tillegg se på hvilke andre behandlingsgrunnlag som er mulige å benytte seg av.

Når jeg skal vurdere praksis hos selskapene (spørsmål 3), vil jeg begrense meg til deler av behandlingen av personopplysninger. Selve innsamlingen av opplysningene og informasjonen som gis i forbindelse med dette blir en sentral del av vurderingen.<sup>7</sup> I tillegg vil jeg se litt på muligheten for å tilegne seg ytterligere informasjon som kunde.

---

<sup>5</sup> Skoleskyss er et gratis kollektivtilbud blant annet til skoleelever som bor langt unna skolen: *Om Skoleskyss*, URL, <http://www.skoleskyss.no/index.php/om-skoleskyss> [lesedato: 20.08.2012].

<sup>6</sup> Boe, Erik (2005): *Grunnleggende juridisk metode – En introduksjon til rett og rettsstenkning*, s. 43.

<sup>7</sup> Dette er viktige momenter knyttet til gyldigheten av et samtykke.

Særlig om muligheten til å trekke tilbake samtykke og eventuelle andre rettigheter den registrerte har.

I vurderingen av selskapenes praksis opp mot rettslige krav (spørsmål 4), vil utgangspunktet være svarene fra utredningen rundt spørsmål 2. Disse vil jeg kryssjekke opp mot observasjonene jeg gjorde for å svare på spørsmål 3.

### 1.3 Personvernperspektiver

Personopplysningslovens formålsparagraf lyder som følger:

*”Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.*

*Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvern hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.”*

Personvern kan fremstå som en litt diffus verdi. Et spørsmål man ofte får høre er; «Hvis jeg ikke har noe å skjule, hvorfor skal jeg frykte at noen følger med?». <sup>8</sup> For å forklare dette vil jeg benytte meg av personvernteori.

Personvernteorien inneholder flere perspektiver på personvern. De forskjellige perspektivene vektlegger forskjellige hensyn som alle kan sies å være en del av det overordnede begrepet personvern. Perspektivene kan ha ganske varierende innfallsvinkel, men har det til felles at de formulerer en metode for å forstå det litt diffuse og abstrakte begrepet personvern. Variasjonen i innfallsvinkel vil gjøre enkelte perspektiver mer aktuelle for visse typer problemstillinger enn andre. I boka Personvern i informasjonssamfunnet, omtaler Schartum og Bygrave de tre viktigste personvernperspektivene: <sup>9</sup>

- Beslutningsperspektivet tar utgangspunkt i at opplysninger om deg er grunnlaget for beslutninger som tas.
- Integritetsperspektivet baserer seg på at du selv skal kontrollere hvor tett innpå deg selv du slipper andre. Din integritet er knyttet til muligheten for å kontrollere avstand til andre.
- Maktperspektivet tar utgangspunkt i hvordan maktforhold påvirkes dersom en part har kunnskap eller opplysninger om en annen.

#### 1.3.1 Beslutningsperspektivet på personvern

Ragnar Dag Blekeli beskriver personvern som «en mulig interesse fra enkeltpersoners side i å utøve kontroll med den informasjon som beskriver dem». <sup>10</sup> Denne interessen begrunner han langt på vei med beslutningsperspektivet, altså at alle personopplysninger om en person kan ende opp med å være grunnlag for en

---

<sup>8</sup> Georg Apenes henviser til dette spørsmålet i forordene til *Personvernrapporten 2010* (2010).

<sup>9</sup> Schartum, Dag Wiese og Lee A. Bygrave (2011): *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*, s. 28.

<sup>10</sup> Blekeli, Ragnar Dag og Knut S. Selmer (1977): *Data og personvern*, s. 21.



beslutning som får konsekvenser for denne personen. Vi snakker her om beslutninger i vid forstand. Både karriere og privatliv kan påvirkes av personopplysninger "på avveie". Kunnskaper om en enkeltperson kan få dramatiske konsekvenser dersom det fører til at vedkommende ikke blir tilsatt eller mister en jobb.<sup>11</sup> Som oftest vil det bli foretatt beslutninger på bakgrunn av personopplysninger om deg som du ikke vil legge merke til, som for eksempel at noen du ikke omgås i særlig stor grad beundrer deg eller ser ned på deg. Like fullt er altså utgangspunktet at du, så langt det er mulig, selv skal kunne påvirke disse beslutningene gjennom å utøve kontroll over dine egne personopplysninger.

### 1.3.2 Integritetsperspektivet på personvern

Den kanskje mest tradisjonelle innfallsvinkelen til personvern er integritetsperspektivet. Integritetsperspektivet er knyttet til ideen om at den enkeltes personvern er delt i forskjellige sfærer som i varierende grad anses som intime.<sup>12</sup> De forskjellige sfærene har varierende grad av "intimitet" fra det ukrenkelige til sfærer av en art som kanskje ikke oppfattes som så veldig private. Dette perspektivet er i større grad preget av statisk definert intimitet enn beslutningsperspektivet.

Schartum og Bygrave deler integritetsperspektivet i 5 former for integritet<sup>13</sup> som kalles:

- Territorial integritet dreier seg om de geografisk avgrensede områdene en person anser som privat. For eksempel ens eget hjem.<sup>14</sup>
- Kroppslig integritet omhandler respekten for egen kropp og informasjon som kan hentes fra denne. For eksempel en blodprøve eller en ubehagelig medisinsk undersøkelse.
- Psykisk integritet beskriver tilfeller der en person blir utsatt for utilbørlig psykisk press. For eksempel lange opphold i varetekt eller at man blir hindret i å notere ned private tanker uforstyrret.
- Kommunikasjonsintegritet er ofte beskyttet av territorial integritet, men gjelder også distansekommunikasjon. Å lese andres e-post eller lytte på deres telefonsamtaler vil typisk være brudd på kommunikasjonsintegritet.
- Informasjonsintegritet er beslektet med kommunikasjonsintegritet, men gjelder både sikring og kontroll av opplysninger om oss selv uavhengig av om vi forsøker å kommunisere den til andre eller ikke.

Vi ser altså at enkelte av disse områdene dreier seg om mer enn bare ren informasjon, men også det å bestemme over hva for eksempel egen kropp blir utsatt for.

---

<sup>11</sup> Også "tilstrekkelig kvalitet på personopplysninger" blir viktig, jamfør popplyl § 1.

<sup>12</sup> Også kjent som Sfæreteorien.

<sup>13</sup> Schartum og Bygrave (2011), s.28.

<sup>14</sup> Altså beslektet med "privatlivets fred" jamfør popplyl § 1.

### 1.3.3 Maktperspektivet på personvern

Dette perspektivet handler om å se på maktforholdet mellom enkeltindividet og andre aktører vedkommende forholder seg til. På den ene siden har hver enkelt et ønske om privatliv, men samtidig møter vi jevnlig kontroll- og reguleringsmekanismer som har behov for informasjon.<sup>15</sup> Mange av disse bruker informasjonen til å utøve makt. Typisk vil en slik diskusjon handle om forholdet mellom enkeltindividet og statens behov for kontroll og regulering, arbeidstakers privatliv og arbeidsgivers styringsrett eller reklame- og markedsstrykk.

Teknologisk utvikling har bidratt til å gjøre dette perspektivet mer aktuelt, rett og slett fordi kontroll og regulering som tidligere var mulig, men tidkrevende, tungvint og dyrt nå er relativt enkelt. Utveksling av data mellom offentlige etater gjør det lettere å ta stikkprøver eller utføre automatisk kontroll med for eksempel skattetrekk, stønader og annen form for støtte eller bidrag. En personlig datamaskin på arbeidsplassen logger det meste en foretar seg og gjør det langt enklere for en arbeidsgiver å kontrollere de ansattes tidsbruk på arbeidsplassen. Dersom en enkeltperson kjenner til at det lagres, loggføres eller på annen måte dokumenteres adferd kan dette føre til at vedkommende oppfører seg annerledes. Ideen om at forventningen om mulig sanksjon endrer adferd kalles "forventningsmakt"<sup>16</sup>. Effekten av forventningsmakt er imidlertid omdiskutert. I boka "*Selektive overblikk*" gjennomgår Heidi Mork Lomell mediedekningen om videoovervåking i Oslo sentrum.<sup>17</sup> Hun viser at det er stor uenighet om, og i hvilken grad, slik forventningsmakt fungerer eller har ønsket effekt.

Elektronisk kartlegging av personlige preferanser vil kunne gi økt kunnskap om målgruppen i markedsføringssammenheng. Direkte elektronisk kommunikasjon som for eksempel e-post og SMS vil kunne bidra til å redusere enkeltindividers motstandsdyktighet mot kjøpsimpulser. Også dette må kunne sies å være en form for makt.

Ofte vil et kontrolltiltak virke fornuftig i seg selv, mens summen av kontrolltiltak potensielt kan skape en uforholdsmessig belastning på den enkeltes personvern. Da kan maktperspektivet være et nyttig verktøy for å forsøke å se på helheten. Skaper summen av tiltak en uforholdsmessig overføring av makt? Sentralt i tolkningen av dette spørsmålet blir også den reelle effekten av kontrolltiltaket.

Dette er ikke en uttømmende liste over områder som omfavnes av maktperspektivet, kun ment for å beskrive og konkretisere teorien. For eksempel nevner Schartum og Bygrave også forholdet mellom fange og fengselsvesen, pasient og helsepersonell, og elev og skole.<sup>18</sup>

---

<sup>15</sup> For eksempel ved at lånekassen kontrollerer inntekt, fartsmålere sjekker at man følger fartsgrensen eller mobilselskapet loggfører informasjon om samtalene dine.

<sup>16</sup> Schartum og Bygrave (2011) s. 35.

<sup>17</sup> Lomell, Heidi Mork (2007), *Selektive overblikk: En studie av videoovervåkingspraksis*. s. 75.

<sup>18</sup> Schartum og Bygrave (2011) s. 36.

#### 1.3.4 Personvernperspektivene i forhold til elektroniske billettsystemer

Det er mulig å bruke alle de tre nevnte personvernperspektiver for å se på innsamling og behandling av personopplysninger i forbindelse med elektroniske billettsystemer.

Beslutningsperspektivet blir for eksempel relevant når kollektivtransportprodusenten får tilgang på statistikk om den enkeltes reisemønster. Denne informasjonen vil typisk føre til at det blir tatt beslutninger knyttet til utforming av rutetilbudet eller målrettede tilbud til enkeltpersoner basert på bruksmønster. Avgjørelsen om å ta i bruk rullende fortau eller innføre rushtidsavgift på kollektivtransport<sup>19</sup> vil være avgjørelser som kan bli påvirket av slik informasjon.

Eksempelet med tilpassede tilbud er også relevant i lys av maktperspektivet. Jo mer informasjon en har om forbruker, jo mer makt har man som markedsfører. En annen måte å utøve makt på er å kontrollere at billetten er gyldig og brukes av rett person. I tilsynsrapporter hos kollektivtransportprodusenter nevnes dette som mulig formål ved behandlingen av personopplysninger.<sup>20</sup> Dette er en mer direkte form for utøvelse av makt (billettkontroll) ovenfor eieren av kortet. Det er også mulig å tenke seg at opplysninger om ditt bevegelsesmønster blir utlevert etter begjæring for politiet, altså at andre enn selve kollektivtransportprodusenten utøver en eller annen form for kontroll av kortets eier.

Schartum og Bygrave skriver at "utgangspunktet for integritetsperspektivet er frie og "ukrenkelige" mennesker."<sup>21</sup> Et slikt utgangspunkt henger sammen med samtykke, altså selvbestemmelse, som utgangspunkt for behandling av personopplysninger. At elektroniske billetter kan vise kundens reisemønster kan delvis sies å være beslektet med territorial integritet etter som hvor man befinner seg i visse tilfeller oppleves som privat. Delvis kan det også beskrives gjennom kommunikasjonsintegritet, da hvor vi beveger oss også potensielt kan si noe om hvem vi kommuniserer med. Mest relevant er nok likevel informasjonsintegritet. Altså ideen om at informasjon om oss selv nyter en viss beskyttelse og at det er opp til den enkelte å regulere hva andre for vite om oss. Hvor vi befinner oss i det offentlige rom, kan neppe sies være opplysninger av meget privat art, men billetten kan også inneholde andre opplysninger. I enkelte tilfeller vil for eksempel en billett knyttet til Skoleskyss<sup>22</sup> kunne inneholde helseopplysninger<sup>23</sup>. Trolig vil de forskjellige opplysningene oppleves som private i varierende grad alt ettersom hvem man spør.

Personvernutfordringen som følger ved bruk av elektroniske billettsystemer er ikke nødvendigvis knyttet til konkret misbruk av personopplysninger. Personvernet kan

---

<sup>19</sup> Hansen Anette Holth, Olav Juven, Knut Erik Solhaug (2012), "Kan bli rushtidsavgift på all kollektivtrafikk i Oslo-området". URL: <http://nrk.no/nyheter/distrikt/ostlandssendingen/1.8079403>

<sup>20</sup> Se for eksempel Datatilsynets kontroll hos Ruter. *Endelig kontrollrapport, 7. mai 2009. Saksnr: 09/00163-15 (2009)*, s. 14.

<sup>21</sup> Schartum og Bygrave (2011) s. 28.

<sup>22</sup> Skoleskyss er nærmere beskrevet og debattert i kapittel 3.4.5.

<sup>23</sup> Det er mulig å få krav på Skoleskyss basert på funksjonshemming, skade eller sykdom, jamfør opplæringslova § 7-3.

være krenket uten at misbruket har funnet sted. Generelt går det an å si at jo flere personopplysninger som registreres og jo flere personer som potensielt blir berørt, jo viktigere er personvernutfordringen.

Det trenger altså ikke være snakk om maktmisbruk<sup>24</sup>, eller frykt for at beslutninger tas på feil grunnlag,<sup>25</sup> for at personvernet krenket. Hver enkelt har en interesse i sitt eget personvern og denne interessen blir med jevne mellomrom utsatt for avveininger mot andre interesser.

### 1.3.5 Interesseteorien

Interesseteorien ble utviklet av Blekeli og Selmer på 70-tallet og har senere blitt videreutviklet og raffinert av blant annet Schartum og Bygrave.<sup>26</sup>

Personvern er i utgangspunktet et overordnet ideal. Idealer kjennetegnes ved at de aldri kan oppnås eller følges 100 % fordi de alltid vil komme i konflikt med andre idealer. Dermed oppstår behovet for interesseavveininger. Interesseavveiningene handler om å identifisere når personvernet må vike for andre behov, enten dette er samfunnets eller enkeltpersoners behov. Sentralt i slike avveininger blir ideen om forholdsmessighet. Av og til vil man også bli nødt til å veie enkelte personverninteresser opp mot hverandre.

Interesseteorien er et forsøk på å kategorisere personvernets idealer i fem hovedinteresser med underliggende krav. Denne konkretiseringen kan brukes som et verktøy som gjør det lettere å vekte personvern hensyn opp mot andre idealer sågar som forskjellige personvern hensyn opp mot hverandre.

Schartum og Bygrave har som nevnt bygget videre på Blekeli og Selmers utgangspunkt og laget sin egen utvidede interesseteori.<sup>27</sup> De fem hovedinteressene er som følger:

- Interessen i å bestemme over tilgangen til opplysninger om egen person
- Interessen i innsyn og kunnskap
- Interessen i opplysnings- og behandlingskvalitet
- Interessen i forholdsmessig kontroll
- Interessen i brukervennlig behandling

Hver av interessene er delt i flere krav som ytterligere konkretiserer hva interessen består av. Enkelte av interessene og deres underliggende krav vil overlappe hverandre, men sammen tegner de tegner et helhetlig bilde og kan være et godt verktøy for tolkning av personvern spørsmål.

---

<sup>24</sup> Ref. maktperspektivet.

<sup>25</sup> Ref. beslutningsperspektivet.

<sup>26</sup> Jfr. *Et bedre personvern* 1997, kapittel 3.

<sup>27</sup> Schartum og Bygrave (2011), Kapittel 2.4.

### 1.3.6 Personopplysning eller ikke?

I popplyl § 2 nr. 1 defineres personopplysninger som ”opplysninger og vurderinger som kan knyttes til en enkeltperson”. I begge casene jeg har sett på har det vært mulig å bruke anonyme versjoner av de elektroniske billettene og selv om det da samles inn detaljerte opplysninger om reisemønster er det altså ikke en personopplysning før det kan knyttes til kortets eier.

Grovt sett kan opplysningene som samles inn og lagres ved bruk av elektroniske billettsystemer i kollektivtransporten deles inn i fire kategorier:

Tabell 1

	Opplysninger som lagres uavhengig av registrering	Opplysninger som lagres om registrerte kort
Opplysninger som er lagret fast om kortet	Type A	Type B
Opplysninger som genereres ved bruk av kortet	Type C	Type D

Med registrerte kort mener jeg kort der innehaveren har knyttet sitt eget navn eller annen identifiserende informasjon til kortet.

Eksempelvis vil opplysninger om billettens varighet (enkeltbillett, periodebillett, klippekort og lignende) være av type A, men vil kun være en personopplysning dersom kortet kan knyttes til eieren. Navn på kortets eier, kontaktinfo eller annen identifiserende informasjon, vil være opplysninger av type B. Opplysninger som genereres ved bruk av kortet vil være de samme på registrerte og uregistrerte kort. Typiske eksempler på slike opplysninger er klokkeslett og holdeplass for bruk av kortet, aktivering av periodebillett eller endringer i kortets saldo. Slike opplysninger vil være av Type C om kortet er uregistrert. Dersom kortet er registrert, vil sistnevnte opplysning kunne klassifiseres som type D.

I utgangspunktet er det kun opplysninger av Type B og D som er personopplysninger og reguleres av popplyl. Det er allikevel mulig å se for seg situasjoner der Type A eller C kan knyttes til en enkeltperson og således gjøre disse til personopplysninger. Dette vil jeg drøfte nærmere i kapittel 3.2 flg.

### 1.4 Utvalg av caser

Jeg har plukket ut Ruter og NSBs Reisekort og Innlandskortet, sistnevnte et samarbeid mellom Oppland Trafikk og Hedmark Trafikk. Av praktiske grunner tok jeg

utgangspunkt i billettsystemer som befinner seg i nærheten av Oslo-området, da dette gjorde det mer realistisk å få gjennomført intervjuer. I østlandsområdet kjenner jeg til tre elektroniske billettsystemer; Ett i Stor-Oslo (Reisekortet), et i Buskerud (uten navn)<sup>28</sup> og et i Hedmark og Oppland (Innlandskortet)<sup>29</sup>.

Reisekortet er det mest omfattende systemet i Norge. Det er også svært aktuelt etter mye medieomtale og oppmerksomhet de siste årene. Ruter har også klaget vedtak fra Datatilsynet inn for Personvernemnda på vegne av flere aktører i bransjen. Dette førte til at arbeidet med en bransjenorm<sup>30</sup> ble satt i gang, og representanter for Ruter var involvert i dette arbeidet. De har med andre ord jobbet en del med spørsmål som er beslektet med problemstillingen min.

Innlandskortet har vært i bruk siden ca. 2006<sup>31</sup>. Inkluderes forløperne Hedmarkskortet og Opplandskortet, har man godt over 10 års erfaring med bruk av elektroniske billettsystemer i området.

Den lange erfaringen med Innlandskortet og dets forløpere vil muligens gi et utvidende perspektiv på Stor-Oslos relativt ferske system. Innlandskortet og Reisekortet har til felles at det foreløpig kun er enkelte billettyper som krever den elektroniske løsningen.<sup>32</sup> Eier av begge systemene har også et uttalt mål om på sikt å basere seg på elektroniske billetter som primærløsning framfor papirbilletter. Disse to systemene er altså sammenlignbare i tilbudet til de reisende, men har forskjellig erfaringsgrunnlag.

Det er også forskjeller i størrelsen på potensiell kundemasse. Totalt i Hedmark og Oppland er det i underkant av 400.000 innbyggere mot Stor-Oslos 1,4 millioner. Innlandskortet har også fått vesentlig mindre medieomtale i riksdekkende presse enn Reisekortet. Hvorvidt slike forskjeller påvirker behandlingen av personvernspørsmål underveis vil kunne gi økt forståelse for valg som er tatt underveis.

## 1.5 Konkret om casene

Både Reisekortet og Innlandskortet har i skrivende stund vært i bruk en del år. Begge tar sikte på at elektroniske kort skal være regelen snarere enn unntaket når de reisende bruker kollektivtilbudet. Begge caser er også resultatet av samarbeid over både fylkesgrenser og mellom forskjellige selskaper. Det er allikevel en del grunnleggende forskjeller som kan være greit å slå fast før vi går videre.

### 1.5.1 Bakgrunnen for Innlandskortet

Innlandskortet er et samarbeid mellom Hedmark Trafikk (HT) og Oppland Trafikk (OT). Begge aktørene er fylkeskommunale bedrifter som har hatt en eller annen form for elektronisk billettering før Innlandskortet ble opprettet. Til sammen dekker de

---

<sup>28</sup> Buskerud kollektivtransport AS, *Velkommen som busspilot på linje 169* (2012), URL: <http://www.bk.no/Billetterogreisekort/Nyttbillettsystem169.aspx>

<sup>29</sup> Innlandskortets hjemmesider, *forside* (2012), URL: <http://www.innlandskortet.no/>

<sup>30</sup> Mer om Bransjenormen i kapittel 6.

<sup>31</sup> Kortet ble gradvis innført i Oppland og Hedmark over flere år.

<sup>32</sup> Ruter har i perioden oppgaven ble skrevet gjort alle billettyper elektroniske med unntak av kupongkortet: Ruters hjemmesider, *kupongkort* (2011), URL: [http://ruter.no/no/billetter/oslo\\_og\\_akershus/kupongkort/](http://ruter.no/no/billetter/oslo_og_akershus/kupongkort/)

kollektivtransporten for ca. 400.000 mennesker.<sup>33</sup> HT og OT har ansvaret for trafikken i hvert sitt fylke, men med enkelte bussruter som krysser fylkesgrensen. Innlandskortet kan brukes på kryss av fylkesgrensen på samtlige ruter hos både HT og OT. Driften av Innlandskortet er organisert gjennom en gruppe kalt "paragraf 27-samarbeidet". Samarbeidet er hjemlet i og har navnet sitt fra kommunelovas § 27.<sup>34</sup> Både HT og OT ser den andre som en 100 % likestilt partner og avgjørelser som angår begge tas i fellesskap i denne gruppen. Den er organisert i en del som tar av seg det meste rundt billetter (teknisk råd) og en del som tar andre administrative avgjørelser. Dersom et spørsmål blir for vanskelig å avgjøre der og da, løftes det opp til et overordnet styre.

### 1.5.2 Bakgrunnen for Reisekortet

Reisekortet er tidligere kjent som (og omtales vanligvis i media som) Flexuskortet eller bare Flexus. Reisekortet er et samarbeid mellom Ruter og NSB. Ruter fungerer som et administrasjonsselskap der Oslo Kommune eier 60 prosent og Akershus fylkeskommune eier 40 prosent. Selve billettsystemet er i sin tid kjøpt inn av AS Sporveisbilletter, som igjen eies av Ruter. Daglig drift av billettsystemer er det imidlertid kollektivtransportproduksjon AS og Interoperabilitetstjenester AS som står for. Førstnevnte eies helt av Oslo Kommune, mens sistnevnte eies 66 prosent av Ruter og resten av NSB.

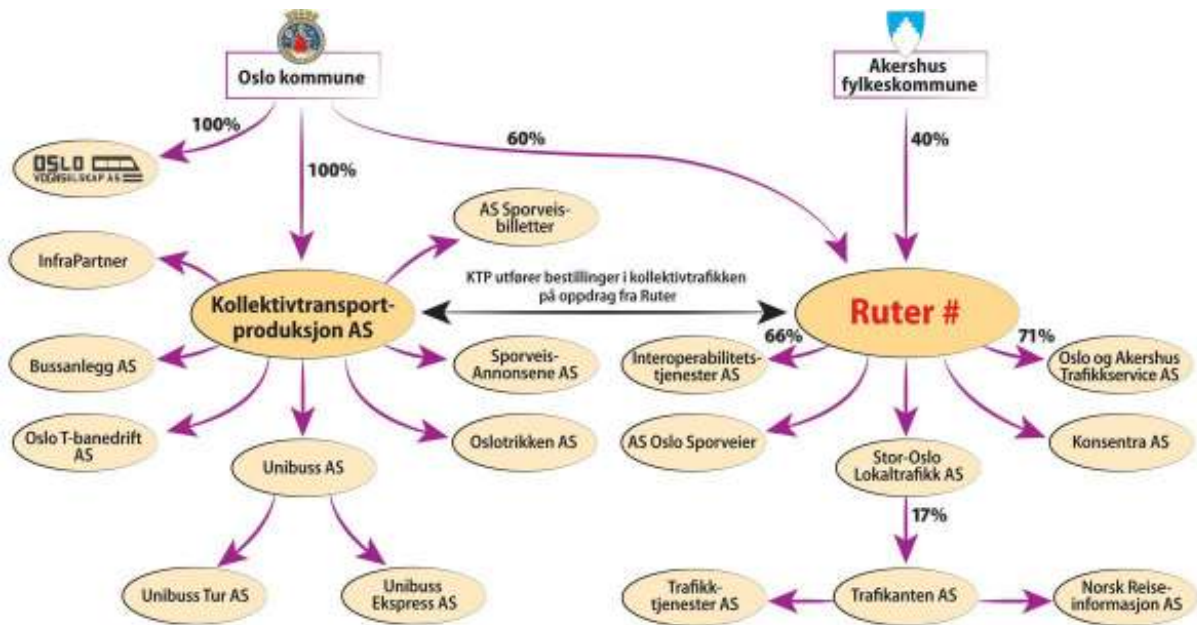
Som tidligere nevnt er kollektivreiser der Reisekortet kan brukes tilgjengelig for nærmere 1,4 millioner mennesker i Oslo og Akershus. I tillegg er det gyldig på NSBs lokaltog. Skal man utenfor grensene for Oslo og Akershus må man imidlertid ha tilleggsbillett i tillegg til Reisekortet. Reisekortet skiller seg altså noe fra Innlandskortet både når det gjelder eierforhold og gyldighetsområde.

---

<sup>33</sup> I følge SSB er det totale innbyggertallet i disse to fylkene ca 380.000. Tallet er et anslag basert på dette og det faktum at det er mye innflyttende studenter i området. *Befolkningsendringer 2010 – 2011*, 2011, tab 4 og 5.

<sup>34</sup> Kommunelovas § 27 åpner for samarbeid mellom kommuner og fylkeskommuner gjennom å opprette egne styrever for å løse felles oppgaver. I dette tilfellet for å kunne tilby et felles kollektivtilbud til begge fylker.



Akershus:<sup>35</sup>

## Slik er kollektivtrafikken i Oslo organisert

De lilla pilene viser hvem som eier de ulike selskapene

Opprinnelig var billettsystemet utviklet av Kollektivtransportproduksjon AS (KTP) som også var systemeier. Grunnet svakheter og feil i systemet ble det gradvis innført over lengre tid. Etter store forsinkelser overtok Ruter ansvaret for systemet i 2009.

## 1.6 Kapitteloversikt

Jeg har nå gått igjennom temaet for oppgaven og deler av den teoretiske konteksten problemstillingen min befinner seg i.

I kapittel 2 vil jeg gå grundigere gjennom arbeidsmetodikken jeg skal benytte meg av. Videre vil jeg gi en oversikt over kildene jeg benytter meg av, inkludert intervjuene jeg skal gjennomføre og sentrale rettskilder. Avslutningsvis vil jeg se litt på potensielle svakheter ved oppgaven.

Jeg skal forsøke å svare på problemstillingens Spørsmål 2 i kapittel 3 ved hjelp av en juridisk gjennomgang av behandlingsgrunnlaget for behandling av personopplysninger. Ettersom begge casene mine benytter seg av samtykke er målet å kunne si noe konkret om hvilke krav som stilles til bruk av samtykke som behandlingsgrunnlag. Jeg vil også gjennomgå enkelte av kravene som følger av personopplysningsloven generelt og utrede hvorvidt noen av de andre behandlingsgrunnlagene kan benyttes. Dette vil gi et godt grunnlag for å svare på Spørsmål 3 senere.

<sup>35</sup> Aftenposten, 17.01.2012.



I kapittel 4 og 5 vil jeg ha en grundigere gjennomgang av praksisen til henholdsvis Reisekortet og Innlandskortet i et forsøk på å besvare Spørsmål 3. Jeg vil hovedsakelig se på prosessen som leder frem til samtykkeerklæringen fra kundene og informasjonen som er tilgjengelig i forbindelse med dette. Dette vil innebære at hovedfokus blir på virksomhetenes hjemmesider der flesteparten av slike henvendelser skjer. Jeg vil også se litt på hvilke muligheter kunden har for å komme i kontakt med virksomhetene og tilegne seg informasjon som er relevant i perioden etter at samtykke er innhentet. Dette vil naturlig nok begrense seg til den delen jeg er i stand til å observere eller har fått innsyn i gjennom intervjuene mine.

Avslutningsvis i hvert av kapitlene 4 og 5 vil jeg sammenligne observasjonene mine med kravene jeg har kommet frem til i kapittel 3. Dette vil i stor grad besvare Spørsmål 4.

I kapittel 6 vil jeg ta en nærmere titt på *Bransjenorm for personvern og informasjonssikkerhet i elektronisk billettering* (heretter omtalt som Bransjenormen). I perioden 2009-2010 hadde Datatilsynet en rekke tilsyn<sup>36</sup> hos aktører som benyttet seg av elektroniske billettsystemer. I etterkant av dette fremmet Ruter en klage til Personvernemnda på vegne av flere av aktørene. Saken kom aldri opp for nemnda, da partene istedenfor utviklet bransjenormen. I skrivende stund er det ment at Bransjenormen skal bli styrende for de fleste tilbydere av kollektivtransport i Norge, men den er enda ikke trådt i kraft. Den er ikke som en del av gjeldende rett å regne, men allikevel for sentral til å overse. Ikke minst fordi den er forhandlet frem av bransjen selv. Kapittelet vil raskt gå gjennom reglene som skisseres opp i normen med fokus på de delene jeg selv har vurdert i kapittel 3-5. Avslutningsvis vil jeg forsøke å oppsummere hvorvidt det er avvik mellom Bransjenormen og det praksisen jeg har avdekket i kapittel 4 og 5.

Kapittel 7 vil være det avsluttende kapittelet. Her skal funnene i kapittel 3-6 oppsummeres og Spørsmål 4 besvares endelig. Her vil jeg også trekke frem eventuelle funn som er spesielt interessante.

## 2.0 Metode

I metodekapittelet vil jeg raskt gjennomgå gangen i arbeidet med oppgaven. Først vil jeg si noe generelt om arbeidsmetodikk. Deretter vil jeg si litt om den juridiske delen av oppgaven. Hvilke metoder jeg har benyttet meg av og hvilke rettskilder som har vært de viktigste. Videre vil jeg redegjøre for intervjuene jeg har gjort, eventuelle dokumenter jeg har fått tilgang på og nettkildene jeg har tatt i bruk. Avslutningsvis vil jeg si noe om svakhetene ved oppgaven og utfordringen som oppstod ved at casene endret praksis underveis.

---

<sup>36</sup> Se for eksempel Datatilsynets kontrollrapporter: 09/00195-9 (Oppland fylkeskommune 2010), 09/00163-15 (Ruter AS 2009), 09/00193-8 (Kolumbus 2010) og 07/01381 (Troms fylkeskommune 2007).

## 2.1 Arbeidsmetodikk

Relativt tidlig i prosessen har jeg avklart gjennom intervjuer med representanter for casene mine at de benyttet seg av samtykke som behandlingsgrunnlag. Deretter har jeg gått gjennom personopplysningslovens krav til behandling av personopplysninger og nærmere inn på selve personopplysningsdefinisjonen. Jeg forsøker her å avklare hva som må regnes som personopplysninger i konteksten kollektivtransport. Videre har jeg tatt for meg de forskjellige behandlingsgrunnlagene og i kartlagt om og når de kan brukes i forbindelse med elektroniske billettsystemer.

Deretter har jeg sett nærmere på de rettslige kravene som stilles til samtykke som behandlingsgrunnlag. Denne delen er i hovedsak en drøftelse av lovens ordlyd og hvordan denne må tolkes på et generelt grunnlag. Dette er muligens den delen av oppgaven der jeg i størst grad har benyttet meg av juridisk metode og gått til rettskildene for å avklare avveiningsspørsmål. Etter dette har jeg forsøkt å ytterligere konkretisere kravene til både behandling av personopplysninger generelt og samtykke spesielt for å få klarhet i hvilke krav jeg kan vurdere casene mine etter.

Videre har jeg kartlagt dagens praksis. Dette skjer primært ved å se på casenes nettsider ettersom begge casene i stor grad baserer seg på at registrering skal skje via nettløsninger. Nettløsningene er altså den primære arenaen for informasjon om samtykket og der selve samtykket gis. Jeg har også sett noe på det som har vært tilgjengelig av skriftlig materiell som for eksempel rutetabeller og informasjonshefter for å se om det er relevant informasjon der. Intervjuene har også bidratt med tilleggsopplysninger som har vært relevante for forståelse av dagens praksis.

Relativt tidlig i prosessen har jeg lest gjennom Bransjenormen, men det er først senere jeg virkelig har forsøkt å analysere innholdet i denne. Jeg har sett på hvorvidt casene mine tilfredsstiller Bransjenormens krav når den trer i kraft.

## 2.2 Juridisk metode

Jeg skal drøfte gjeldende rett på et område som er lite utforsket. Det er skrevet en hel del om personvernteori, personopplysningsloven, behandlingsgrunnlag og samtykke, men stort sett på overordnet nivå. Spørsmål knyttet til personvern og elektroniske billettsystemer er ikke utredet noe sted i rettssystemet.

I mitt arbeid med å utrede hva som er gjeldende rett har jeg benyttet meg av juridisk metode slik det er beskrevet av Erik Boe.<sup>37</sup> Utgangspunktet for de juridiske drøftelsene i kapittel 3 er personopplysningsloven med forskrift, og dermed har jeg også blitt nødt til å se på forarbeidene til disse.<sup>38</sup> Jeg har brukt Norsk Lovkommentar om personopplysningsloven som en inngangsport til tolkningen av lov og forskrift. I de tilfeller der jeg har hatt behov for ytterligere presisjon i tolkningen av begreper har jeg sett på EUs personverndirektiv og dets fortale. I arbeidet med å tolke disse

---

<sup>37</sup> Boe, Erik (2005) Del IV.

<sup>38</sup> Sentrale forarbeider er *Offentlige persondatasystem og personvern* (1975), *Et bedre personvern* (1997) og *Individ og integritet* (2009).

rettskildene har jeg også benyttet meg av støttelitteratur. Spesielt sentrale kilder har vært Blekeli og Selmers *Data og personvern*, Schartum og Bygraves *Personvern i informasjonssamfunnet* og Ottesen og Blixruds *Personvern i finanssektoren*.

Jeg har også sett på Datatilsynets kontrollrapporter<sup>39</sup> innen aktuelle områder. Dette er supplert med relevante avgjørelser i Personvernemnda. Jeg har ikke funnet noen avgjørelser som går direkte på billettsystemer og kollektivtransport,<sup>40</sup> men både Personvernemndas avgjørelser og rapportene fra Datatilsynet er blitt brukt som referansepunkter når jeg har kartlagt og konkretisert gjeldende rett. Kanskje særlig relevant har dette vært i avveiningsspørsmål.

Utover dette har jeg også lest en del utredninger og høringsuttalelser som for eksempel Datatilsynets høringsuttalelser om personopplysningsloven<sup>41</sup> og Fornyings- og administrasjonsdepartementets nettsider om personvern<sup>42</sup>. Dette er kilder som ikke går direkte på tolkningen av gjeldende rett, men som er nyttige for å oppnå en bedre helhetlig forståelse for fagområdet.

## 2.3 Intervjuene

Jeg har gjennomført i alt 4 intervjuer med 6 personer. Intervjuene har vært semi-strukturerte intervjuer der hovedtemaer er tenkt gjennom på forhånd og det har blitt stilt åpne spørsmål. I egne notater har jeg hatt supplerende lister over spørsmål jeg har ønsket svar på. I utgangspunktet har det vært snakk om intervjuer med enkeltpersoner, men ved to av anledningene har det vært to personer til stede. Ved disse to anledningene har jeg primært behandlet en av disse som intervjuobjekt, mens den andre har vært der for å supplere med informasjon i spørsmål som det originale intervjuobjektet ikke hadde kunnskap om. Alle intervjuene har vart mellom 70 og 90 minutter og er registrert ved at jeg har tatt fortløpende notater på laptop.

Intervjuobjektene stilling hos aktørene har selvsagt også gjort dem til personer mer eller mindre robust kunnskap om personvernspørsmål, men det er først og fremst i kraft av deres erfaringer de er plukket ut.

De 5 respondentene har vært:

- Svend Eric Wandaas, Personvernansvarlig<sup>43</sup> og juridisk rådgiver hos Ruter.
- Helge Olsen Bye, IT-medarbeider hos Hedmark Trafikk.
- Kjell Arne Olsen, IT-medarbeider hos Hedmark Trafikk.
- Bjørn Rune Holmen, Teamleder IKT hos Oppland Trafikk.

---

<sup>39</sup> Nærmere bestemt rapportene, Endelig kontrollrapport 21.03.2009 (Oppland fylkeskommune), Endelig kontrollrapport 02.04.2009 (Kolumbus), Endelig kontrollrapport 25.10.2007 (Troms fylkeskommune) og Endelig kontrollrapport 7. mai 2009 (Ruter AS).

<sup>40</sup> Den eneste klagesaken jeg kjenner til ble aldri behandlet da partene kom til enighet og formulerte den nevnte bransjenormen.

<sup>41</sup> Apenes, Georg og Hågen Ljøgodt (2009): *Høringsuttalelse - etterkontroll av personopplysningsloven*.

<sup>42</sup> Fornyings- og administrasjonsdepartementet, *Hva er personvern?*, URL: <http://www.regjeringen.no/nb/dep/fad/tema/personvern/hva-er-personvern.html?id=448290>

<sup>43</sup> Wandaas er også registrert som Ruters personvernombud hos Datatilsynet.

- Stine Fredriksen fra markedsavdelingen hos Oppland Trafikk.

I tillegg har jeg intervjuet Atle Årnes hos Datatilsynet.

På forespørsel motsatte Wandaas seg at intervjuet ble tatt opp. Dette var også det første intervjuet jeg gjorde og planen var å gjennomføre opptak på samtlige intervjuer.

Opprinnelig hadde jeg avtale med Olsen Bye hos Hedmark Trafikk, men han inviterte på eget initiativ sin kollega Olsen til å være til stede og supplere. På grunn av plassering inne på Byes kontor og lydforholdene ellers var det umulig å få til opptak av noen særlig kvalitet. Begge to var til stede under hele intervjuet.

Under intervjuet hos Oppland Trafikk ble Fredriksen kalt inn på møterommet for å svare på spørsmål om kundecontact og de fremtidige planene for billettsystemet. Utover dette foregikk mesteparten av intervjuet med Holmen alene. På bakgrunn av at ingen av intervjuene hadde blitt tatt opp hittil, valgte jeg å heller ikke gjøre opptak av dette. Dette fordi jeg nå var blitt vant med en intervjuform og fordi jeg ønsket at situasjonene skulle være så sammenlignbare som mulig.

Intervjuet med Årnes ble foretatt hos Datatilsynet og etter at de andre intervjuene var fullført. Dette intervjuet inneholdt naturlig nok en del andre spørsmål enn de tidligere og handlet i større grad om bransjen som helhet og Bransjenormen.

Intervjuene har innledningsvis dreiet seg rundt temaer som billettsystemets historikk og planer for videre utvikling. Videre har vi snakket om hvilket behandlingsgrunnlag de benytter seg av, bakgrunnen for dette valget og tekniske spesifikasjoner som for eksempel hva slags informasjon som lagres, hvor og hvor lenge det lagres og hvem som har tilgang på opplysningene. Jeg har også stilt spørsmål om hva slags informasjon som gis til kundene og hvilke tilbud som er et resultat av behandling av personopplysninger. Avslutningsvis har de fortalt om sitt forhold til Bransjenormen og eventuelt samarbeid med Datatilsynet.

Intervjuet med Atle Årnes skiller seg fra denne malen. Her har intervjuet i større grad fokusert på gjeldende rett, vanlige trender i bransjen og Bransjenormen.

## 2.4 Dokumentstudier

Det har vært begrenset tilgang til dokumenter fra casene mine. Bransjenormen har vært tilgjengelig på nett og det har også enkelte brev og vedtak som var foranledningen til initiativet som ble Bransjenormen.

Fra Innlandskortet fikk jeg utlevert en mal for databehandleravtalen deres. Innlandskortet gav meg også en utskrift av hvilke opplysninger som lagres ved bruk av kortet samt et eksempel på en kvittering som viste de 8 siste transaksjonene på et testkort.

Fra Ruter har jeg fått tilgang på noe skriftlig materiell som kundene kan finne blant annet på Trafikanten. Materiellet inneholdt generell informasjon om billettsystemet.

Jeg har også fått varierende grad av muntlig gjengivelse og mulighet til å se vedleggene til Bransjenormen, men aldri fått med meg en kopi å se nærmere på. Disse vedleggene henvises til i Bransjenormens tekst med ujevne mellomrom, men de er ikke vedtatt sammen med normen og følgelig ikke lagt ut på nettet eller gjort offentlig tilgjengelig på annen måte.

## 2.5 Nettkilder

De mest sentrale nettkildene har selvsagt vært casenes egne hjemmesider. Mesteparten av kapitlene 4 og 5 er basert på observasjoner herfra. I tillegg til å kartlegge nettsidenes struktur og personvernrelatert informasjon, har jeg også forsøkt å registrere egne elektroniske billetter for å følge hele prosessen fra A til Å. Etter at kortet er registrert har jeg også testet muligheten for å trekke tilbake samtykket.

Jeg har også funnet en del artikler som omtaler billettsystemene. Disse artiklene har først og fremst hjulpet meg å spore opp nyttig tilleggsinformasjon som å slå fast når de forskjellige systemene ble tatt i bruk, oppbygning av organisasjonene som drifter systemene og så videre.

Wikipedia har også vært i bruk, men stort sett for å finne statistiske fakta (innbyggertall og lignende) og som en pekepinn til andre relevante kilder.

Mange av rettskildene og de juridiske drøftingene jeg har brukt er tilgjengelige på offentlige nettsider som, for eksempel personvernemnda.no, rettsdata.no og regjeringen.no.

## 2.6 Begrensninger og svakheter ved metoden

Intervjuobjektene mine har hatt varierende kompetanse. Hos en aktør snakket jeg med personvernombudet og et annet sted en mann som primært har IT-teknisk kompetanse. Dette gjør det vanskeligere å sammenligne intervjuene og få grundige svar på alle typer spørsmål. Det hendte for eksempel rett som det var at de tolket tekniske spørsmål som juridiske og omvendt.

Enkelte av intervjuobjektene har ikke vært til stede under hele prosessen med å implementere billettsystemene. Dette har selvsagt gjort det vanskeligere å få klarhet i systemenes historikk. Jeg har forsøkt å kompensere for dette ved å stille oppfølgingsspørsmål og få dem til å avklare usikkerheter med sine kolleger.

Intervjuene bar innimellom preg av at kontrollene fra Datatilsynet var friskt i minnet. Jeg opplevde å måtte bruke tid på å betrygge intervjuobjektene mine, for å unngå at de kom i forsvarsposisjon. Det er en mulighet for at de ikke snakket så fritt som de ville gjort om jeg hadde snakket med dem i forkant av kontrollene. Alle intervjuobjektene stilte seg til disposisjon i ettertid både for presiseringer og sitatsjekk, så i den grad det har vært hensiktsmessig har jeg kunnet tett igjen hull fra intervjuene gjennom dette.

Det finnes svært begrenset rettspraksis på dette området og opprettelsen av en bransjenorm gjør det lite trolig at det vil bli skapt ytterligere prejudikater i overskuelig framtid. Det er vanskelig å vurdere i hvilken grad retningslinjene i Bransjenormen gir den samme praksis som en eventuell avgjørelse etter en rettstvist, eller hvorvidt den bærer preg av å være et kompromiss mellom kollektivtransportprodusentenes behov og Datatilsynets tolkning av regelverket.

Bransjenormen ble utviklet samtidig med arbeidet med denne oppgaven. Den var varslet klar i juli 2011, men ble ikke lansert før nærmere årsskiftet 2011/2012. Flere av temaene jeg hadde sett for meg å diskutere når gjeldende rett skulle kartlegges, blir langt på vei overflødige når hele bransjen sammen med den største premissleverandøren på området blir enige om hvordan praksis skal være. Dette førte også til at Ruters klagesak i Personvernemnda aldri ble behandlet. Allikevel kan en utredning av gjeldende rett være interessant. Bransjenormen må også begynne seg innenfor rammene loven setter. Jeg kan imidlertid ikke late som om mine vurderinger ikke blir påvirket av innholdet i Bransjenormen. Å lene seg på vurderingene som allerede er gjort kan være både fristende eller noe man ender opp med å gjøre underbevisst.

### 2.6.1 Hovedutfordringen underveis

I intervjuer med representanter for Innlandskortet i mars, ble jeg gjort oppmerksom på at kravene stilt i Bransjenormen muligens ville sørge for at registrerte kort ble faset ut som alternativ. Det ble ansett som for krevende i forhold til gevinsten og fortsatt operer med registrerte kort og det ble derfor vurdert om all registrering av personopplysninger skulle opphøre. Bransjenormen skulle offisielt tre i kraft 1. juni, og i den forbindelse skulle rutiner gjennomgå.<sup>44</sup> Tidlig i mai måned ble registreringsrutinen på innlandskortet.no stengt. Dette var før jeg hadde fått tak i et eksemplar av Innlandskortet. Planen var å gjennomgå registreringsprosessen og sikre skjermdump av denne underveis. Ettersom tjenesten ikke lenger var tilgjengelig, ble det derfor umulig å dokumentere selve inngåelsen av samtykke i detalj. En eventuell gjennomgang ville også kun analysere "noe som har vært" og således ha redusert verdi.

Denne utfordringen oppsto etter at ruter.no var gjennomgått og analysert og like før oppgaven skulle avrundes. Det var derfor i seneste laget å endre problemstilling eller oppgavens struktur drastisk.

Jeg har valgt å vurdere nettsidene til Innlandskortet på samme måte som Ruters nettsider så langt det har vært mulig. Flere av de viktigste momentene i forkant av en samtykkeerklæring er fortsatt mulige å vurdere. Selv om vurderingen ender opp med å handle om "noe som har vært" vil de fortsatt være interessante som sammenligningsgrunnlag for lignende løsninger. Mine vurderinger i kapittel 6.6, der

---

<sup>44</sup> Også Ruter opererte med deadline til 1.juni for gjennomgang av egne rutiner i lys av Bransjenormen.

jeg ser nærmere på hva casene kan gjøre for å tilpasse seg Bransjenormen, er også med på å utvide relevansen for undersøkelsene mine.

Også nettsidene til Ruter har endret seg under skrivingen av denne oppgaven. Etter intervjuet med representanten Wandaas har nettsidene endret seg i større eller mindre grad hele tre ganger. Endringene er dog ikke så fundamentale som hos Innlandskortet og registreringsprosessen som er vurdert er den siste utgaven.

### 3. 0 Juridiske drøftelser

I dette kapittelet skal jeg svare på problemstillingens Spørsmål 2 ved å utrede lovens krav til de behandlingsgrunnlag som benyttes av casene mine. Allerede før intervjuene ble gjennomført, fikk jeg bekreftet svaret på Spørsmål 1 fra begge casene. Ettersom behandlingsgrunnlaget til begge caser i all hovedsak<sup>45</sup> er samtykke, vil hovedfokus i kapittelet være dette. Jeg vil først redegjøre for de mest sentrale lovbestemmelsene for behandling av personopplysninger og plassere behandlingsansvaret i virksomhetene.

Deretter vil jeg utrede når det behandles personopplysninger ved bruk av elektroniske billetter og når opplysningene må anses som anonyme.

Jeg vil så se på behandlingsgrunnlagene. Først vil jeg begrunne hvorfor samtykke er det foretrukne behandlingsgrunnlaget. Videre vil jeg utrede muligheten hvorvidt nødvendighetsgrunnene kan begrunne behandling av personopplysninger i forbindelse med elektroniske billettsystemer.<sup>46</sup> Her vil jeg også kort gå gjennom behandlingsgrunnlaget for billettkontroll og Skoleskyss.

Til slutt vil jeg redegjøre for hvilke krav som stilles til et gyldig samtykke.

#### 3.1 Sentrale bestemmelser i personopplysningsloven

Som tidligere nevnt er personopplysningslovens formål "*å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger*".<sup>47</sup>

En personopplysning er definert som en opplysning eller vurdering som kan knyttes til en enkeltperson.<sup>48</sup> Å behandle personopplysninger innebærer "enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter".<sup>49</sup>

Personopplysningsloven gjelder for behandling av personopplysninger der elektroniske hjelpemidler tas i bruk, opplysningene lagres i et register samt alle former for kameraovervåking. Det er imidlertid definert enkelte unntak i popplyl § 3.

---

<sup>45</sup> For unntaket om Skoleskyss og billettkontroll, se kapittel 3.4.5. og 3.4.4

<sup>46</sup> Selvsagt med en forutsetning at konteksten er noenlunde lik casene mine.

<sup>47</sup> Jfr. popplyl § 1.

<sup>48</sup> Jfr. popplyl § 2 nr.1

<sup>49</sup> Sitatet er fra § 2 nr.2.



Videre vil eventuell særlovgivning ha forrang foran personopplysningsloven.<sup>50</sup> Jeg skal ikke beskrive unntakene uttømmende, og vil nøye meg med å konstatere at elektronisk behandling av personopplysninger i utgangspunktet faller innunder lovens virkeområde<sup>51</sup> og at drift av kollektivtransport med tilhørende billettsystem ikke kommer innunder noen av unntakene i § 3. Det er også gjort enkelte unntak for å sikre ytringsfriheten i § 7, men dette vil ikke være relevant i forhold til elektroniske billettsystemer. I § 4 står det at loven gjelder for behandlingsansvarlige som er etablert i Norge. Begge mine caser er dette.

Lovens § 2 nr 4. definerer den behandlingsansvarlige som *”den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes”*.

Behandlingsansvaret plasseres der instruksjonsmyndigheten i organisasjonen befinner seg. Dersom noen behandler personopplysningene på vegne av den behandlingsansvarlige<sup>52</sup> vil denne person eller organisasjon være definert som databehandler<sup>53</sup>.

Vilkår for å behandle personopplysninger defineres i popplyl §§ 8 og 9. § 9 gjelder vilkårene for å behandle sensitive personopplysninger.<sup>54</sup> Som nevnt i kapittel 3.2 er ikke dette relevant for bruken av elektroniske billetter på kollektivtransport og dermed er det § 8 vi skal forholde oss til. Som jeg har vært inne på tidligere er det tre mulige behandlingsgrunnlag for å behandle personopplysninger. Disse vil jeg drøfte utfyllende i kapitlene som følger.

Popplyl § 11 inneholder grunnkrav til behandling av personopplysninger. Foruten å henvise til vilkårene i popplyl §§ 8 og 9 stilles det her krav til at opplysningene bare kan benyttes til det angitte formålet<sup>55</sup> med behandlingen. Underforstått må altså all behandling av personopplysninger ha et definert formål før innsamling kan finne sted. Formålet må være *”saklig begrunnet i den behandlingsansvarliges virksomhet”*<sup>56</sup> og opplysningene som benyttes må ha et minimum av relevans i forhold til å oppfylle formålet.<sup>57</sup> I tillegg gir § 11 en plikt til å sikre opplysningenes kvalitet.<sup>58</sup> Sistnevnte innebærer både å sikre tilstrekkelighet og relevans samt at opplysningene er korrekte og oppdaterte. Her presiseres det også at opplysninger ikke kan lagres lengre enn nødvendig.

---

<sup>50</sup> Ref. lex specialis-prinsippet.

<sup>51</sup> Jfr. popplyl §3 bokstav b.

<sup>52</sup> Altså noen som den behandlingsansvarlige i utgangspunktet ikke har direkte instruksjonsmyndighet over.

<sup>53</sup> Jfr. popplyl § 2 nr. 5.

<sup>54</sup> Sensitive personopplysninger er definert i popplyl § 2 nr 8.

<sup>55</sup> Formål er ikke definert i loven, men popplyl § 2 nr. 4 definerer den behandlingsansvarlige som den som fastsetter formålet. Popplyl § 11 forutsetter at personopplysninger kun benyttes til det på forhånd angitte formål.

<sup>56</sup> Jfr. popplyl § 11 bokstav b.

<sup>57</sup> Jfr. popplyl § 11 bokstav d.

<sup>58</sup> Jfr. popplyl § 11 bokstav e.



I § 13 gis det en forpliktelse til behandlingsansvarlig for å ”*sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet*”. Altså sikre at opplysningene er beskyttet mot innsyn fra uvedkommende og uautorisert endring samt at opplysningene er tilgjengelige for det angitte formålet når nødvendig. Sistnevnte vil nødvendigvis innebære et krav om oppetid for servere, databaser og lignende.

Popplys § 13 3. ledd og § 15 gir den behandlingsansvarlige plikt til å påse at en eventuell databehandler<sup>59</sup> følger bestemmelsene i loven og at vedkommende langt på vei har de samme plikter som den behandlingsansvarlige. I § 13 3. ledd legges det særlig vekt på informasjonssikkerhet. Dette innebærer at en databehandleravtale<sup>60</sup> må gi behandlingsansvarlig en viss instruksjonsmyndighet over databehandler.

I popply § 14 gis den behandlingsansvarlige en forpliktelse til å skape rutiner for internkontroll som skal kontrollere etterlevelsen av loven. Særlig nevnes sikring av opplysningenes kvalitet. Tiltakene skal kunne dokumenteres.

Ved innsamling av personopplysninger plikter den behandlingsansvarlige å informere den registrerte om en rekke forhold, blant annet hva formålet med behandlingen er og hvilke rettigheter den registrerte har. Informasjonsplikten reguleres av popply §§ 19-22 med unntak definert i § 23. Den registrertes rettigheter til innsyn er definert i § 18. Det følger av § 27 at den registrerte har krav på å få rettet mangelfulle opplysninger og av § 28 at opplysninger i visse tilfeller kan kreves slettet.

Enhver behandling av personopplysninger skal meldes til Datatilsynet.<sup>61</sup> Denne meldingen skal blant annet inneholde formålet med behandlingen. Datatilsynet kan velge å gi unntak fra meldeplikten dersom en behandlingsansvarlige utnevner et personvernombud. Dette følger av personopplysningsforskriftens § 7-12 som også inneholder en beskrivelse av personvernombudets plikter.

I Ot.prp. nr. 92 (1998-99) drøftes muligheten for å opprette ”bransjevisse atferdsnormer” gjennom et samarbeid mellom Datatilsynet og representanter for den enkelte bransje.<sup>62</sup> Drøftingen lander på at dette er en gunstig måte å tilpasse en generell lov til de enkelte bransjers behov.

Datatilsynet har jobbet med flere aktører innenfor kollektivtrafikk og vedtatt en bransjenorm<sup>63</sup> vinteren 2011. Ettersom bransjenormen er såpass fersk og ikke har rukket å få konsekvenser for hvordan casene mine drifter billettsystemene enda, vil

---

<sup>59</sup> En databehandler er definert i popply § 2 nr. 5 som ”den som behandler opplysninger på vegne av den behandlingsansvarlige”.

<sup>60</sup> Altså en avtale som regulerer forholdet mellom behandlingsansvarlig og databehandler.

<sup>61</sup> Jfr. popply § 31.

<sup>62</sup> Ot.prp. nr. 92(1998-99) Om lov om behandling av personopplysninger (personopplysningsloven), kapittel 6.10

<sup>63</sup> Bransjenorm - for personvern og informasjonssikkerhet i elektronisk billettering (2011).

jeg holde denne utenfor diskusjonen foreløpig. Jeg vil imidlertid komme tilbake til bransjenormen i kapittel 6.

Det er selvsagt flere bestemmelser i loven enn de jeg har vært inne på i denne oppsummeringen. Blant annet defineres andre rettigheter for den registrerte i lovens kapittel IV samt at kapittel VII gir tilleggsregler i forbindelse med kameraovervåking. Dette kapittelet bør likevel gi en oversikt over lovens oppbygning og de bestemmelsene som er mest relevante for oppgaven.

### 3.2 Å knytte en opplysning til en person

I forrige kapittel slo jeg i første avsnitt fast at personopplysninger som blir behandlet i et elektronisk billettsystem kommer inn under lovens virkeområde.<sup>64</sup> Som jeg har vært inne på er en personopplysning definert som "opplysninger og vurderinger som kan knyttes til en enkeltperson".<sup>65</sup>

I noen tilfeller er dette meget lett å identifisere. Dersom det er registrert navn, fødselsnummer eller andre tydelige identifikatorer på en profil knyttet til kortet vil alle opplysninger som kan knyttes til kortet bli knyttet til kortets eier. Alle opplysningene som genereres ved bruk av kortet vil dermed være personopplysninger. På skalaen mellom denne typen åpenbare eksempler på at det er personopplysninger som behandles og helt anonyme opplysninger, finnes det en rekke opplysninger som er i en slags gråsone.

Om kortet er knyttet til en adresse med kun en beboer registrert, er dette trolig nok til at kortet inneholder personopplysninger. Om adressen er en boligblokk vil det være mer usikkert om kortet kan sies å kunne knyttes til en person. Begge disse eksemplene handler om direkte tilknytning. Altså at opplysningen registrert på kortet, enten den er entydig eller har en mer vag tilknytning, kan knyttes direkte til en person. Det kan også tenkes en mer indirekte tilknytning, for eksempel at opplysningene er knyttet til en elektronisk billetts serienummer og billetten blir funnet i kundens lommebok. Teoretisk har man da tilgang på reisedataene og mulighet til å knytte dem til en enkelt person. Det er nærliggende å se for seg at disse opplysningene knyttes til en person ved å slå opp i en kundedatabase. En mer usannsynlig tilknytning kan skje gjennom kombinasjon av store mengder data eller fra forskjellige kilder. For eksempel ved at man visuelt overvåker et område og sammenligner denne observasjonene med reisedata. Over tid vil det bli mulig å identifisere personen som er opphav til reisedataene. Et sted på skalaen mellom enkle åpenbare tilknytninger og mer søkte muligheter for en tilknytning må det trekkes en grense for når tilknytningen "skaper" en personopplysning.

Opplysninger som genereres av eller kan knyttes til elektroniske billetter der kundens kontaktinformasjon er registrert på kortet, heretter omtalt som registrerte kort, er uten

---

<sup>64</sup> Jfr. popplyl § 3

<sup>65</sup> Jfr. popplyl § 2 nr. 2

tvil personopplysninger. Hvorvidt en uregistrert elektronisk ihendehaverbillett genererer personopplysninger er derimot mer usikkert.

### 3.2.1 Opplysninger knyttet til uregistrerte kort

Selv om det er nok at en opplysning "kan knyttes til en person"<sup>66</sup> for at den skal være en personopplysning er det ikke slik at alle tenkelige teoretiske tilknytninger vil skape en personopplysning i lovens forstand. Loven sier ikke noe direkte om hvor denne grensen går og derfor vil jeg se nærmere på hvorvidt bruk av uregistrerte kort genererer personopplysninger.

I denne drøftelsen forutsetter jeg at kortet har en eller annen form for unik identifikator. Som regel vil dette være et serienummer. Dersom man slår opp dette serienummeret i kollektivtransportfirmaets databaser, vil man kunne få en oversikt over blant annet reisene gjort med kortet. Slik jeg har forstått det er en slik teknisk løsning relativt vanlig.

Det er som nevnt nok at det eksisterer en mulighet for kobling mellom opplysningen og personen. Koblingen trenger altså ikke ha funnet sted for at det skal være en personopplysning. Ved hjelp av serienummer vil koblingen mellom selve kortet og opplysninger generert av kortet<sup>67</sup> være rimelig åpenbar. Jeg vil derfor ikke gå nærmere inn på dette. Spørsmålet blir om koblingen mellom kortet og kortets eier er "sterk nok" til at opplysningene knyttet til kortet kan kalles personopplysninger i lovens forstand. Koblingen oppstår ved at vedkommende er i besittelse av kortet eller at kortet er oppbevart på et sted som gjør at man med rimelig stor sikkerhet vet hvem som er kortets eier.<sup>68</sup>

I boka Personvern i finanssektoren, omtaler Christine Ask Ottesen og Katrine Berg Blixrud indirekte identifisering av personer og slår fast at "Det følger [...] av forarbeidene at selv en begrenset identifikasjonsmulighet er tilstrekkelig."<sup>69</sup> Altså at opplysninger knyttet til et kundennummer, telefonnummer eller lignende er å regne som en personopplysning. I personopplysningslovens forløper, personregisterloven, står dette eksplisitt.<sup>70</sup> Også i personverndirektivet, som er grunnlaget for personopplysningsloven, presiseres det i Artikkel 2 at tilknytningen kan være indirekte.<sup>71</sup> Selv om personopplysningsloven ikke presiserer dette, betyr ikke det at loven representerer et avvik i forhold til direktivet. I lovens forarbeider fastholdes denne definisjonen.<sup>72</sup>

---

<sup>66</sup> Min understreking.

<sup>67</sup> Disse vil typisk være lagret sentralt på en server med kortnummeret som identifikator.

<sup>68</sup> For eksempel i eierens jakkelomme eller private nattbordsskuff.

<sup>69</sup> Ottesen, Christine Ask og Katrine Berg Blixrud (2010): *Personvern i finanssektoren*, s. 36

<sup>70</sup> *Personregisterloven*, § 1 annet ledd.

<sup>71</sup> *Personverndirektivet*, Artikkel 2 bokstav a.

<sup>72</sup> Presiseringen om indirekte tilknytning dukker opp både i "*Et bedre personvern*" (1997) s. 131 og Ot.prp. nr. 92 (1998-1999), s. 101.

Det å knytte en opplysning til en person innebærer at man med rimelig sikkerhet må vite hvem som er opphavet til opplysningene eller hvem opplysningen sier noe om. I boka "Personvern i Informasjonssamfunnet" argumenterer Schartum og Bygrave for at dersom en opplysning kan knyttes til 4-5 mulige forskjellige personer vil tilknytningen være for usikker og neppe som personopplysning å regne.<sup>73</sup> De hevder imidlertid at dersom opplysningen knyttes til en husstand bestående av samme antall personer vil personopplysningslovens formålsparagraf kunne gi en annen tolkning. Dette fordi formålet med loven er "å beskytte den enkelte mot at personvernet blir krenket" og at opplysninger blir "behandlet i samsvar med grunnleggende personvern hensyn, herunder [...] privatlivets fred".<sup>74</sup> Hensynet til privatlivets fred tilsier altså en videre tolkning når man beveger seg inn i det man må anse som en privat sfære. I tilfellet med uregistrerte kort, vil informasjonen ikke kunne omhandle opplysninger generert i en husstand eller andre områder som må regnes som privat og vil stort sett si noe om bevegelser i det offentlige rom. Det er derfor ikke grunnlag for å hevde at hensynet til privatlivets fred taler for en videre tolkning.

Dersom en kunde med et uregistrert kort henvender seg til et kundesenter med kortet i hånden, vil man med rimelig stor sikkerhet anta at opplysningene dreier seg om vedkommende.<sup>75</sup> Dette fordi svært få andre vil ha interesse av disse opplysningene<sup>76</sup> og kortet som regel vil oppbevares i en lommebok eller tilsvarende privat sted. I et slikt tilfelle vil opplysningen om bruk av kortet og personens identitet være sammenstilt, og opplysningene er å regne som personopplysninger. Det kan dermed argumenteres for at muligheten for at en slik form for sammenstilling vil skje, samt at identifiseringen vil være sikker nok, til at vi snakker om personopplysninger.

***"whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"***

Fortalen til EUs personverndirektiv nr. 26

I spørsmålet om hvorvidt en opplysning som enda ikke er knyttet direkte til en identitet er en personopplysning, blir det viktig å vurdere sannsynligheten for at tilknytningen skjer og hvor vanskelig det er å gjennomføre en slik sammenstilling. I denne sammenheng vil vurderingen av vanskelighet måtte inneholde både eventuell arbeidsinnsats, kostnadsnivået eller andre forhold som kan hindre sammenstillingen fra å bli gjennomført.

---

<sup>73</sup> Schartum og Bygrave (2011) s.124.

<sup>74</sup> Jfr. popplyl § 1

<sup>75</sup> Dette er praksis hos Ruter i dag dersom henvendelsen gjelder klage på defekt billett eller lignende.

<sup>76</sup> Det er for eksempel ikke det samme potensialet for svindel eller lignende som et bankkort på avveie.

Forarbeidene til personopplysningsloven<sup>77</sup> trekker frem en norsk oversettelse av fortalen til EUs personverndirektiv. Der heter det at hvorvidt sammenstillingen kan skje skal vurderes i lys av "alle hjelpemidler [...] som det er rimelig å ta i bruk for å identifisere vedkommende, enten av den behandlingsansvarlige eller av en annen person". Både den engelske originalen og den norske oversettelsen tilsier en viss dualitet i tolkningen. På den ene siden understreker bruken av ordet "alle" at tolkningen bør være rimelig vid. Samtidig settes det en begrensning i rimelighet. Bruken av ordet "likely" i den engelske utgaven taler også for en sannsynlighetsvurdering.

Rimelige og sannsynlige metoder og hjelpemidler for å knytte en opplysning til en identitet, og på den måten gjøre opplysningene til personopplysninger, må nok begrenses til personer som på lovlig vis og ved hjelp av lovlige metoder kan gjennomføre tilknytningen. Schartum og Bygrave bruker en hacker som eksempel på en person som i de fleste tilfeller vil falle utenfor denne rimelige mulighetsvurderingen.<sup>78</sup> Det er også verdt å merke seg at den mulige sammenstillingen kan foretas av andre enn den behandlingsansvarlige, jamfør den siterte fortalen over.

Schartum og Bygrave nevner kort muligheten for at en opplysning som ikke er en personopplysning i utgangspunktet kan bli det dersom opplysningen fremstår i en ny kontekst.<sup>79</sup> For eksempel ved at opplysningene lekkes og dermed gjøres tilgjengelig for flere personer. En slik av/på-tolkning av personopplysningsdefinisjonen må nødvendigvis forutsette at endringen som utgjør forskjellen i utgangspunktet anses som svært usannsynlig. Under mitt intervju med Svend Eric Wandaas forklarte han at Ruter hadde en tilsvarende forståelse av en liknende situasjon. Ruter etterspør kun de opplysningene de trenger fra kundene for å oppfylle formålet med å ha registrerte kort. Det hender allikevel at kunden på eget initiativ gir ekstra opplysninger i relativt omfattende grad. Selv om dette ikke er noe Ruter selv har tatt initiativet til, blir denne informasjonen behandlet som en personprofil<sup>80</sup> etter popplyl § 21. En slik situasjon gir behandlingsansvarlig ekstra plikter i forhold til å informere den registrerte. Dette er ikke et spørsmål om hvorvidt vi snakker om personopplysninger eller ikke, men det er et eksempel på at også aktører i bransjen mener opplysningene kan endre karakter dersom forholdene endrer seg.

### 3.2.2 Kortets tilknytning til den registrerte

Opplysninger kan altså bli personopplysninger om de kan knyttes til en person. Muligheten for en tilknytning må være der, men ikke for diffus eller usannsynlig.

---

<sup>77</sup> Ot. Prp. Nr. 92 (1998-1999) s. 101.

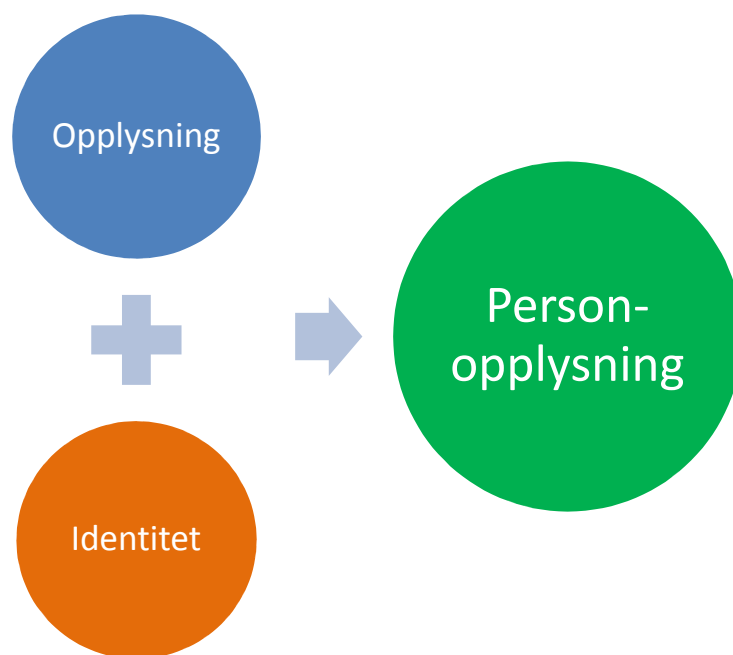
<sup>78</sup> Schartum og Bygrave (2011) s. 127.

<sup>79</sup> Schartum og Bygrave (2011) s. 126.

<sup>80</sup> I loven er dette beskrevet som "personprofiler som er ment å beskrive atferd, preferanser, evner eller behov, f eks som ledd i markedsføringsvirksomhet".

Dette kan beskrives som å koble en opplysning (eller flere) til en identitet. Jeg har forsøkt å illustrere dette i figur 3 under. En opplysning (blå sirkel) kan for eksempel være informasjon om forrige gang en elektronisk billett (et kort) ble validert eller hva slags billett kortet inneholdt. Identiteten (oransje sirkel) kan være en opplysning som i seg selv sier noe om hvem den handler om, som for eksempel navn registrert på kortet, eller en opplysning som gir en sterk tilknytning til identiteten, som for eksempel et telefonnummer eller fødselsnummer. Identiteten kan også være en observasjon, som for eksempel opptak fra et overvåkningskamera<sup>81</sup> som viser valideringen på samme klokkeslett som opplysningen ble lagret. Når disse to blir koblet eller kan kobles, har vi altså en personopplysning (grønn sirkel).

Figur 3



I tilfellene med uregistrerte kort vil opplysningene befinne seg hos kollektivselskapets server/datasystem.<sup>82</sup> Identiteten vil være knyttet til at kortet befinner seg på eierens person eller oppbevares på en annen måte som tilsier at det tilhører vedkommende. Kortnummeret alene vil ikke si noe om eieren av kortet. Slik jeg ser det, er det to realistiske scenarier som tilsier at opplysningene knyttet til serienummeret er, eller kan bli, koblet til en identitet. Scenario 1 innebærer at kortets eier henvender seg til de som er i besittelse av opplysningene om kortet. Scenario 2 innebærer en henvendelse fra en annen person som ikke er den opplysningene sier noe om, men som har kortet og kjenner til hvem som var bruker av kortet da opplysningene ble generert. La oss kalle vedkommende ihendehaver av kortet.

---

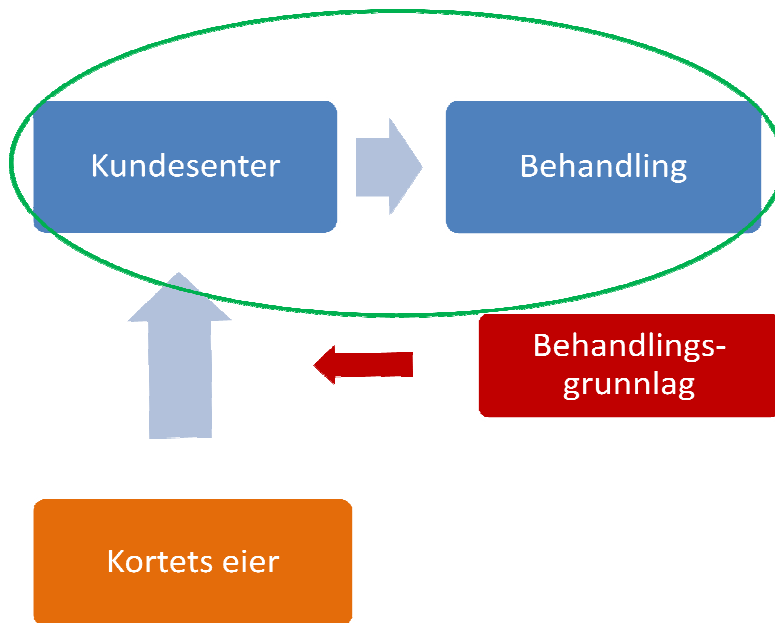
<sup>81</sup> "Rene kognitive prosesser, som å gjenkjenne en person på et bilde, kan være tilstrekkelig for å oppnå identifikasjon." Ottesen og Blixrud (2010), s. 35.

<sup>82</sup> Alternativt i datasystemet til databehandler som drifter dette for dem.

### 3.2.3 Scenario 1

Jeg har forsøkt å lage en grafisk fremstilling av scenario 1 i figuren under. Fargekodene er bevisst beholdt fra Figur 3 slik at for eksempel oransje fortsatt representerer identiteten.

Figur 4



I denne situasjonen vil kortets eier ved sitt nærvær tilføre opplysningene identitet. Representanten for kundesenteret<sup>83</sup> (for enkelhets skyld kalt behandlingsansvarlig<sup>84</sup>) vil så sammenstille disse opplysningene, og dermed behandle personopplysninger i lovens forstand. Den behandlingsansvarlige vil med rimelig stor grad av sikkerhet kunne anta at henvendelsen gjelder vedkommendes eget kort, og dermed også ha en identitet å knytte til kortet. Selv om vedkommende ikke skriver ned eller lagrer identiteten til kortets eier, vil det skje en sammenstilling der og da. Om den behandlingsansvarlige forklarer eller viser frem noen av opplysningene generert av kortets bruk, vil det også skje en utlevering av personopplysninger.<sup>85</sup> At opplysningene blir definert som personopplysninger er avhengig av prosessen som er markert med en grønn ring i figuren.<sup>86</sup> Det er uklart om muligheten for at denne situasjonen kan oppstå tilsier at vi snakker om personopplysninger hele tiden. I motsatt fall, altså at opplysningene hos kundesenteret i utgangspunktet ikke er personopplysninger, blir de det under denne behandlingen. I tilfelle vil behandlingen basere seg på en direkte henvendelse, og sannsynligvis basert på et behov, fra kortets eier. Det oppstår dermed en situasjon som kan sies å skape et selvstendig

<sup>83</sup> For eksempel en ansatt i skranken på et billettkontor.

<sup>84</sup> Vedkommende vil være en representant for behandlingsansvarlig eller en databehandler som opererer på vegne av behandlingsansvarlig.

<sup>85</sup> Både utlevering og sammenstilling er behandling av personopplysninger jmfør popplyl § 2.

<sup>86</sup> Altså at "kundesenter" mottar identiteten og behandler opplysninger.

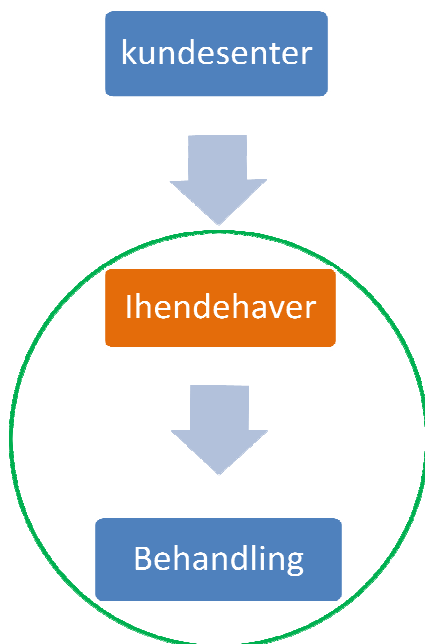
behandlingsgrunnlag for denne behandlingen (markert med rødt i figuren). Dette skjer enten ved at henvendelsen defineres som et samtykke,<sup>87</sup> eller ved at kortets eier krever en rettighet og dermed utløser behandlingsgrunnlag i en av nødvendighetsgrunnene.<sup>88</sup> I et slikt tilfelle vil opplysningene slutte å være personopplysninger etter at behandlingen er gjennomført, forutsatt at det ikke registreres tilleggsopplysninger som kan lette identifisering. Dersom opplysningene er personopplysninger hele tiden vil behandlingsgrunnlaget og formålet med behandlingen være definert på forhånd.

En vurdering av denne situasjonen i lys av rimelighets- og sannsynlighetskriteriene vil avgjøre om dette er personopplysninger fra før av, eller om henvendelsen skaper en situasjon som nevnt i kapittel 3.2.1 som endrer opplysningene til personopplysninger ved henvendelse. Før jeg går nærmere inn i denne vurderingen, vil jeg skissere opp det andre scenarioet.

### 3.2.4 Scenario 2

I scenario 2 vil en annen enn kortets eier henvende seg til kundesenteret. Den behandlingsansvarlige har ikke noen reell mulighet for å kontrollere hvem som er kortets rettmessige eier. Med mindre ihendehaveren aktivt opplyser om dette, vil situasjonen oppleves som identisk med scenario 1. Den behandlingsansvarlige vil dermed måtte oppføre seg som om det er den registrerte som henvender seg. I realiteten vil situasjonen være nærmere illustrasjonen i figuren under.

Figur 5



<sup>87</sup> Jfr. popplyl § 8, første ledd.

<sup>88</sup> Sannsynligvis popplyl § 8 bokstav a.



Behandlingsansvarlig vil tro at han behandler personopplysningene til kortets eier, men i realiteten ikke ha koblet opplysningene til rett identitet. Rent teknisk vil behandlingsansvarlig kunne sies å behandle feilaktige personopplysninger om ihendehaver. Om vi forutsetter at ihendehaver kjenner til korteiers identitet vil imidlertid ihendehaveren være i stand til knytte opplysningene til identiteten etter at de er overlevert fra behandlingsansvarlig. Dette vil selvsagt skape en utfordring for informasjonssikkerheten, men det er ikke det jeg skal se på i dette scenarioet.

Selve sammenstillingen, og dermed behandlingen av personopplysninger om kortets eier, vil i realiteten foregå et annet sted enn i Scenario 1. Dette er markert med en grønn ring i Figur 5. Behandlingen gjennomføres av en annen enn behandlingsansvarlig og ikke på vegne av behandlingsansvarlig.<sup>89</sup> Det kan være opplysningene dermed blir behandlet uten tillatelse fra korteier. Behandlingen blir da en følge av "ulovlig innsats" og utenfor rimelighetskriteriet fra fortalen til personverndirektivet. Alternativt er det er snakk om en ny behandling av en ny behandlingsansvarlig som opererer med samtykke fra kortets eier. At det er for en ny behandling og ny behandlingsansvarlig å regne forutsetter at dette ikke er definert som personopplysninger før koblingen mellom opplysning og identitet skjer. I motsatt fall er kundesenteret fortsatt behandlingsansvarlig, men mest sannsynligvis uvitende om at dette er en annen situasjon enn i Scenario 1.

Det er også mulig å se for seg at ihendehaveren identifiserer seg som en annen enn den registrerte og hevder å ha fullmakt/samtykke. Dette vil i realiteten være umulig å etterprøve, men vi må anta at behandlingsansvarlig ikke leverer ut opplysninger til en person som selv har erkjent at hun ikke er den registrerte.

Tidligere har jeg hevdet at det er rimelig å anta at vedkommende som henvender seg er kortets eier/bruker og dermed blir det urimelig å mene at behandlingsansvarlig skal ha et annet utgangspunkt enn at dette er tilfellet. Årsaken til at dette er lite sannsynlig, er at en slik elektronisk billett vil som regel befinne seg i en lommebok, kortholder, jakkelomme eller lignende som tilhører kortets eier. Trolig vil det også være relativt lite å vinne på å tilegne seg en annens reiseopplysninger.

Om ihendehaveren besitter kortet på lovlig vis, er det rimelig å anta at det foreligger et samtykke mellom ihendehaver og kortets eier som jeg har vært inne på over. Behandlingsansvarlig vil likevel ha en forpliktelse til ikke å utlevere opplysningene til annen person enn kortets eier, men vil mest sannsynlig ikke ha muligheten til å kontrollere dette.

### 3.2.5 Drøftelse

Jeg har nå sett på to mulige scenarier som skisserer hvordan et uregistrert kort kan knyttes til både en identitet og personopplysninger generert av kortet. Det avgjørende spørsmålet er hvorvidt denne mulige koblingen er "sterk" nok til å tilfredsstille

---

<sup>89</sup> Altså ikke en databehandler, jamfør popplyl § 2 nr. 5.

definisjonen i popplyl § 2 nr 1. Hvorvidt opplysningene er for personopplysninger å regne i forkant av disse scenariene er avgjørende for den behandlingsansvarliges forpliktelser.<sup>90</sup> Dersom reiseopplysningene må anses som personopplysninger uavhengig av om henvendelsen skjer eller ikke, vil dette kreve formulering av et formål<sup>91</sup> med behandlingen, et gyldig behandlingsgrunnlag<sup>92</sup> og tilstrekkelig informasjonssikkerhet. I motsatt fall vil opplysningene i utgangspunktet ikke ha status som personopplysninger, men få det i det en slik kobling oppstår. Som tidligere nevnt innebærer dette at muligheten for å koble opplysning og identitet anses som meget usannsynlig.

Det er nok ikke riktig å hevde at en henvendelse fra en kunde er urealistisk eller urimelig. Det er allikevel flere elementer som taler for at dette ikke er en enkel vurdering. Faktorer som alvorlighetsgraden av personvernkrenkelsen, kostnad eller innsats som kreves for sammenstilling og mulig gevinst ved sammenstilling bør alle være en del av helhetsvurderingen.

Scenario 2 tar for seg en henvendelse som for behandlingsansvarlig fremstår som identisk med Scenario 1. Henvendelsen er enten basert på ulovlig tilegnelse av kortet,<sup>93</sup> eller en samtykkebasert handling på vegne av kortinnehaver.<sup>94</sup> Dermed er vi nødt til å se nærmere på tilfellet i Scenario 1. En slik henvendelse vil typisk skje dersom det oppstår en feil, eller kortets eier mener noe er feil. I tilfeller der kortet fungerer som det skal og kortets eier føler seg trygg på at hun har fått alt hun har krav på vil det sannsynligvis ikke være noen grunn til å møte opp på kundesenteret. Personopplysningslovens formål er "å beskytte den enkelte mot at personvernet blir krenket".<sup>95</sup> I dette eksempelet er det neppe sannsynlig at behandlingsansvarlig er i stand til å koble opplysning med identitet uten korteiers ønske. Om den registrerte selv tar initiativet til behandlingen kan det neppe sies å være en krenkelse av hennes personvern. Dersom vi forutsetter at opplysningen om hennes identitet ikke lagres, vil ikke sammenstillingen kunne skje i ettertid uten et tilsvarende initiativ. Det er neppe slik at lovens formål passer spesielt godt på situasjonen over og taler nok ikke for en vid tolkning av personopplysningsbegrepet i dette tilfellet. Det vil også mest sannsynlig være begrenset med informasjon å hente ut om reisemønsteret til vedkommende.<sup>96</sup> Å sammenstille opplysningene vil neppe by på store kostnader eller være vanskelig, men det er trolig lite å vinne på å beholde sammenstillingen av denne informasjonen for den behandlingsansvarlige. Det er dermed vanskelig å

---

<sup>90</sup> Både opplysninger lagret på selve kortet og opplysninger lagret sentralt og er tilgjengelige gjennom kortets serienummer.

<sup>91</sup> Som beskrevet i popplyl § 11 bokstav b jamfør. § 2 nr. 4.

<sup>92</sup> Jfr. popplyl §§ 8 og 9.

<sup>93</sup> Og dermed en utenfor rimelighetskriteriet i fortalen.

<sup>94</sup> En slik henvendelse vil ikke være annerledes enn Scenario 1 i forhold til opplysningenes tilknytning til identiteten.

<sup>95</sup> Jfr. popplyl § 1.

<sup>96</sup> Opplysningene skal bare lagres en gitt periode før sletting. Ifølge Datatilsynet gjelder dette også reiseopplysninger generert av "anonyme" kort.

hevde at alvorlighetsgrad av personvernkrenkelse eller mulig gevinst ved overtramp taler for en vid tolkning av lovteksten.

Personvernemnda har ved en tidligere anledning definert en liknende situasjon som behandling av personopplysninger. I deres sak<sup>97</sup> om passering i bompengeringer definerer nemnda passeringsdata som personopplysninger fordi hver enkelt passeringsbrikke kan knyttes til bilens nummerskilt. Også i de tilfeller der selve brikken ikke er knyttet til noe navn eller abonnement. Denne vurderingen har ikke nødvendigvis tilstrekkelig overføringsverdi til eksempelet med elektroniske billetter. I eksempelet med bomringer ble alle biler tatt bilde av. Koblingen mellom kortnummer og reiseopplysninger er ikke tilgjengelig via et offentlig tilgjengelig oppslagsverk<sup>98</sup>.

I tilfellet elektroniske billettsystemer er kortets eier i besittelse av den eneste nøkkelen for å knytte opplysningene til identiteten. Den behandlingsansvarlige har det overordnede ansvaret for å sikre informasjonssikkerheten. Likevel er det rimelig å plassere noe av ansvaret hos innehaver av "nøkkelen". Eieren av et minibankkort har ansvar for å ikke oppbevare kort og kode sammen og enhver som benytter seg av en innloggingstjeneste (for eksempel Altinn) har til en viss grad ansvar for å hindre uvedkommende å få tak i påloggingsinformasjonen sin. Som jeg skal komme nærmere inn på i kapittel 3.3 er deler av hensikten med personopplysningsloven å gi den registrerte en viss grad av selvbestemmelse.<sup>99</sup> At den registrerte selv besitter "nøkkelen til koblingen" er i tråd med en slik tankegang.

Som jeg har vært inne på er formålet med loven "å beskytte den enkelte mot at personvernet blir krenket". Muligheten for en grov krenkelse eller alvorlig konsekvens tilsier en videre tolkning av hva som må regnes som personopplysning og dermed også strengere krav til informasjonssikkerhet. Stavanger Aftenblad hadde i 2010<sup>100</sup> et oppslag om en kvinne som ville sjekke hvorfor samboerens kort var sperret og fikk utlevert reisedata for tre og et halvt år tilbake. En slik krenkelse av personvernet må anses som relativt omfattende, men trolig vil ikke dette være mulig dersom kollektivselskapet overholder sletteplikten etter popplyl § 28. Om vi forutsetter at den behandlingsansvarlige følger lovbestemmelsene, vil det begrense potensielt skadeomfang betraktelig. Alvorlighetsgraden må anses som rimelig lav og sjansen for at koblingen skjer relativt sett liten. Trolig vil det være lite å tjene på å bryte egne sikkerhetsrutiner eller sammenstille opplysningene på egen hånd for den behandlingsansvarlige.

### 3.2.6 Konklusjon

En konklusjon som innebærer tilstedeværelse av personopplysninger på ihendehaverkort vil forutsette et behandlingsgrunnlag for drift av disse kortene. Et

---

<sup>97</sup> PVN - 2005 - 11, *Klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner*.

<sup>98</sup> Eier av bilen kan enkelt slås opp via motorvognregistreret med utgangspunkt i bilens registreringsnummer.

<sup>99</sup> Dette er begrunnelsen for at samtykke er det prioriterte behandlingsgrunnlaget.

<sup>100</sup> Stavanger Aftenblad (2010), s. 4.

slikt behandlingsgrunnlag vil enten være samtykke eller nødvendighetsgrunnene. Dette vil ansvarliggjøre behandlingsansvarlig i langt større grad og styrke kravene til informasjonssikkerheten, men neppe gi den registrerte større grad av kontroll. Ettersom risikoen for personvernkrænkelser i utgangspunktet er lav er det også usikkert om sikkerheten reelt sett vil bli noe særlig forbedret av dette.

Dersom dette behandlingsgrunnlaget er samtykke,<sup>101</sup> vil det i praksis ikke lenger være valgfritt for kunden å ha kontakt med kollektivselskapet i forbindelse med bruk av billetten. Trolig vil manglende kobling mellom kort og identitet gjøre det vanskeligere å knytte kortet til eieren og til en viss grad øke informasjonssikkerheten. Rent praktisk vil det utgjøre liten forskjell for den registrerte, men det vil definitivt oppleves som en tettere kobling mellom en selv og opplysningene kortet genererer om man kontaktes for å avgi samtykke. Kravet til et slikt behandlingsgrunnlag vil dermed kunne fungere mot sin hensikt.

Samtidig vil en tolkning der personopplysningene oppstår ved henvendelse spare den behandlingsansvarlige for en rekke forpliktelser og mulig komplikasjoner i den daglige driften av systemet. En slik tolkning vil sørge for at det er i den behandlingsansvarliges interesse å gjøre koblingen mellom kortnummer og korteier så perifer som mulig<sup>102</sup> og dermed i praksis kunne øke informasjonssikkerheten.

Kundens mulighet til selv å kontrollere tilgang til opplysningene og kontakt med kollektivselskapet bør veie tungt. Trolig vil hensiktsmessighetshensyn tale for å legge til grunn en tolkning der personopplysninger oppstår ved henvendelsen.

### 3.3 Samtykket har prioritet

Vilkårene for å behandle personopplysninger er regulert i popplyl §§ 8 og 9. Loven skisserer opp tre mulige rettslige grunnlag for behandling av personopplysninger.<sup>103</sup> Det må enten foreligge et samtykke, en lovhjemmel eller en «nødvendighetsbegrunnelse»<sup>104</sup>. Det eksisterer ingen eksplisitt lovhjemmel for innsamling av personopplysninger om kollektivreisende. Da gjenstår samtykke og nødvendighet som mulige behandlingsgrunnlag.

---

<sup>101</sup> I kapittel 3.3 vil jeg vise at samtykke trolig vil måtte prioriteres.

<sup>102</sup> For eksempel ved å ha slette- eller anonymiseringsrutiner på overflødige opplysninger som ikke er personopplysninger.

<sup>103</sup> Se også: KLAGESAK 2004/01: Klage på Datatilsynets vedtak om vilkår om samtykke for konsesjon for delstudie 1 og 2 – Statens Arbeidsmiljøinstitutt – STAMI.

<sup>104</sup> Som beskevet i popplyl § 8 a-f.

Vilkårene for å behandle alminnelige personopplysninger finner vi som nevnt i personopplysningslovens § 8:

*”§ 8. Vilkår for å behandle personopplysninger*

*Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for*

*a) å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,*

*b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse,*

*c) å vareta den registrertes vitale interesser,*

*d) å utføre en oppgave av allmenn interesse,*

*e) å utøve offentlig myndighet, eller*

*f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.”*

Om man tolker første ledd bokstavelig, er de tre mulige behandlingsgrunnlagene tilsynelatende likeverdige. Det er lite som tyder på noen ”innbyrdes rangering” mellom behandlingsgrunnlagene i personopplysningsloven. I Datatilsynets høringsuttalelse – Etterkontroll av personopplysningsloven har tilsynet likevel kommet med følgende uttalelse<sup>105</sup>:

*”Når det gjelder lovgivers intensjon om at samtykke vil være det foretrukne behandlingsgrunnlag, kan ikke Datatilsynet se at det er et særskilt behov for å klargjøre dette nærmere. Også på dette området er forvaltningspraksis klar, samtykke er utgangspunktet for behandling av personopplysninger.”*

At samtykke er foretrukket behandlingsgrunnlag finner vi støtte for i forarbeidene.<sup>106</sup> Her kommer det fram at muligheten for å bruke grunnlagene i popplyl § 8 bokstav a-f er tilstrekkelig, det må samtidig være noe som hindrer bruk av samtykke.

Dette synet støttes i Personvernemndas sak om STAMI.<sup>107</sup> Nemnda argumenterer her for at selv om innhenting av samtykke er tungvint eller kostbart, skal det gjøres en forholdsmessighetsvurdering der samtykke fortsatt skal tillegges vekt som det foretrukne behandlingsgrunnlaget. I samme sak omtales samtykke som ”hovedregelen”. Også i personopplysningsforskriften finner vi en presisering i retning

<sup>105</sup> Apenes og Ljøgdott (2009), s. 17.

<sup>106</sup> Ot.prp. nr. 92 (1998-99), s.108.

<sup>107</sup> KLAGESAK 2004/01.

av at samtykke prioriteres.<sup>108</sup>

Samtykket som behandlingsgrunnlag overfører makt fra den behandlingsansvarlige til den registrerte. I høringsuttalelsen påpeker også Datatilsynet at noe av hensikten med personopplysningsloven var å gi "enkeltindividet [...] større råderett over egne personopplysninger".<sup>109</sup>

I en konkret sak om Ruters bruk av det elektroniske billettsystemet Flexus, hevder Datatilsynet at «enhver må kunne reise kollektivt og anonymt.»<sup>110</sup> Implisitt i dette kravet ligger kravet om valgfrihet for enkeltindividet. Denne saken ble riktignok klaget inn til Personvernemnda, men ble lagt på is<sup>111</sup> i påvente av resultatet av samtaler mellom blant andre Datatilsynet, Ruter og norske veimyndigheter.<sup>112</sup> Resultat ble den tidligere omtalte Bransjenormen.

### 3.3.1 Foreløpig oppsummering om samtykke

Det er liten tvil om at samtykke er det foretrukne behandlingsgrunnlaget. Terskelen for å sette samtykket til side er høyere enn om de tre mulige behandlingsgrunnlagene skulle vært sidestilt. I den eneste saken jeg kjenner til som omhandler elektroniske billettsystemer har også Datatilsynet kommet med en uttalelse som implisitt forutsetter samtykke som behandlingsgrunnlag. Begge casene mine baserer seg på samtykke og dermed er det fristende å kun forholde seg til dette behandlingsgrunnlaget i oppgaven. For at nødvendighetsgrunnene i popplyl § 8 bokstav a-f skal kunne anvendes må det være uforholdsmessig dyrt og/eller vanskelig å innhente samtykke. Selv om det i utgangspunktet må meget tungtveiende grunner til for å sette samtykke til side, bør vi neppe avvise muligheten for at forholdene hos et kollektivselskap kan være av en slik art. Jeg vil derfor gå gjennom kravene loven stiller til et gyldig samtykke før jeg kan konkludere med sikkerhet.<sup>113</sup> Før jeg gjennomgår disse kravene vil jeg først se på de forskjellige nødvendighetsgrunnene og utrede hvorvidt de er anvendelige dersom samtykke av en eller annen grunn skulle være vanskelig å gjennomføre.

### 3.4 Nødvendighetsgrunnene

Personopplysningene som samles inn via de elektroniske billettsystemene jeg har sett på er ikke sensitive etter popplyl § 2 nr. 8.<sup>114</sup> Dermed blir det behandlingsgrunnlaget i popplyl § 8 det er aktuelt å se nærmere på. Personopplysningslovens § 8 inneholder nødvendighetsgrunnene i bokstavene a-f.

---

<sup>108</sup> I merknaden til personopplysningsforskriftens § 7-27.

<sup>109</sup> Apenes og Ljøgodt (2009), s.4.

<sup>110</sup> Zachariassen, Espen (2010), "Flexus: – En syretest på personkartlegging".

<sup>111</sup> Jfr. brev av 09.11.2012 fra Datatilsynet til Personvernemnda. Ellertsen, Kim og Jørgen Skorstad (2010): *Vedrørende stansing av saker til behandling i Personvernemnda*.

<sup>112</sup> Involverte parter er fylkeskommunene og deres respektive kollektivtransport selskap, Kollektivtransportforeningen, Interoperabilitetstjenester AS, Ruter, NSB, Vegdirektoratet, Samferdselsdepartementet og Datatilsynet. Ifølge e-post fra Datatilsynet 02.05.2011.

<sup>113</sup> Mer om denne vurderingen i kapittel 3.7.

<sup>114</sup> Sensitive personopplysninger er her definert uttømmende og ingen av opplysningene som samles inn er av typen som ramses opp i popplyl § 8 nr. 2 bokstav a-e.

Aller først vil jeg gå gjennom de nødvendighetsgrunnene som neppe vil være aktuelle i forbindelse med drift av kollektivtransport og dets elektroniske billettsystemer. Det er vanskelig å se for seg at slike systemer genererer personopplysninger man er avhengig av å behandle for "å ivareta den registrertes vitale interesser". Det vil neppe være snakk om "å utøve offentlig myndighet" heller.<sup>115</sup> Det ville i så fall kreve at det fattes vedtak<sup>116</sup> på bakgrunn av opplysningene. I forarbeidene kommer det frem at å "oppfylle en rettslig forpliktelse" skal innebære "plikt som er hjemlet i lov eller forskrift, eller som følger av dom eller forvaltningsvedtak"<sup>117</sup>. Det er selvfølgelig mulig å se for seg teoretiske situasjoner hvor noe slikt kan forekomme, for eksempel ved at kollektivselskapet får krav fra domstol om å utlevere opplysninger til politiet i forbindelse med etterforskning. Dette vil imidlertid ikke være knyttet til det opprinnelige formålet med behandlingen.

Det kan nok diskuteres hvorvidt det å drifte kollektivtransport er "å utføre en oppgave av allmenn interesse" eller ikke, jamfør popplyl § 8 bokstav d. Debatten om hvorvidt den allmenne interessen er tungtveiende nok i lovens forstand er omfattende. Personlige billetter neppe er en forutsetning for å kunne gjennomføre driften av kollektivtransporttilbudet.<sup>118</sup> Derfor vil jeg ikke gå nærmere inn på denne drøftelsen.

Det er derfor rimelig trygt å konkludere med at det primært er bokstavene a og f i popplyl § 8 som må ses nærmere på når jeg skal vurdere om nødvendighetsgrunnene kan brukes.

### **3.4.1 Formålet med behandlingen**

For å kunne ta stilling til hvorvidt nødvendighetsgrunnene kan begrunne behandling av personopplysninger, er avgjørende hva personopplysningene skal brukes til. Dermed må jeg først kartlegge formålet med behandlingen.<sup>119</sup> I følge popplyls § 11 bokstav b, er all behandling av personopplysninger nødt til å ha et "uttrykkelig angitt formål som er saklig begrunnet i den behandlingsansvarliges virksomhet". Jeg har ikke funnet meldinger til Datatilsynet om behandling av personopplysninger i meldingsdatabasen<sup>120</sup> som dreier seg om kartlegging av reisemønstre eller kundeinformasjonen til billettinnehavere.<sup>121</sup>

---

<sup>115</sup> Skoleskyss og gjennomføring av billettkontroll kan muligens begrunnes i denne nødvendighetsgrunnen, men disse tilfellene tar jeg spesielt i henholdsvis kapittel 3.4.5 og 3.4.4.

<sup>116</sup> Jfr. forvaltningsloven § 2 bokstav a og b.

<sup>117</sup> Ot. Prp. 92 (1998-1999), s. 109.

<sup>118</sup> Unntaket er muligens skoleskyss som jeg drøfter i 3.4.5.

<sup>119</sup> Jfr. popplyl § 11 første ledd bokstav b.

<sup>120</sup> Datatilsynets meldingsdatabase, *meldingssøk*.

<sup>121</sup> Jeg har gjort søk på Fara As, Sporveien, Ruter, Kollektivtransportproduksjon, interoperabilitetstjenester, Innlandskortet, Hedmark trafikk, Oppland trafikk, Hedmark fylkeskommune og Oppland fylkeskommune.

Datatilsynet har hatt kontroller hos Oppland Trafikk, Ruter, Kolumbus og Tromskortet.<sup>122</sup> Alle disse kontrollene har hatt elektronisk billettering og behandling av personopplysninger som tema. I de aktuelle sakene er følgende formål opplyst til Datatilsynet:

- Å administrere kundemassen.
- Å kontrollere bruken av kortet.
- Å etablere statistikk til bruk ved planlegging av rutetilbud.
- Å kontrollere at periodebilletten kun benyttes av en person.
- Å kontrollere at periodebilletten kun benyttes av rett person.
- Å få bekreftet at kunden har gyldig billett.
- Å gi kunden refusjon i forbindelse med ubenyttet kort.
- Å belaste kundens reisekonto.
- Avregning mellom selskaper.

Alle rapportene er skrevet i løpet av 2009 og 2010. Det er viktig å presisere at samtlige av disse kontrollene avdekket en praksis om Datatilsynet ikke mente var god nok. Det er derfor naturlig å anta at det har skjedd endringer frem til i dag.

I intervju med representanter for Innlandskortet og Reisekortet har jeg fått opplyst følgende formål:

- Rekonstruksjon av tapte kort.
- Feilsøking i datasystemet
- Håndtering av kunder/bedre kundeservice
- Fakturering av abonnementstjenester

Jeg har sortert disse formålene inn i to kategorier etter hvorvidt de kan gjennomføres uten å knytte kortet til et navn eller på annen måte knytte det til en person.

Gjennomførbart uten registrering av kort:	Avhengig av at en identitet knyttes til kortet:
Å etablere statistikk til bruk ved planlegging av rutetilbud.	Å kontrollere at periodebilletten kun benyttes av en person.
Å gi kunden refusjon i forbindelse med ubenyttet kort.	Å kontrollere at periodebilletten kun benyttes av rett person.

---

<sup>122</sup> *Endelig kontrollrapport 21.03.2009* (Oppland fylkeskommune), *Endelig kontrollrapport 7. mai 2009* (Ruter AS), *Endelig kontrollrapport 02.04.2009* (Kolumbus) og *Endelig kontrollrapport 25.10.2007* (Troms fylkeskommune).



Avregning mellom selskaper.	Å få bekreftet at kunden har gyldig billett.
Å kontrollere bruken av kortet.	Å belaste kundens reisekonto.
Feilsøking i datasystemet.	Rekonstruksjon av tapte kort..
	Håndtering av kunder/bedre kundeservice.
	Fakturering av abonnements tjenester.

Når det gjelder formålet "å administrere kundemassen" er ikke dette kategorisert og heller ikke med i den senere drøftelsen. Det er ingen entydig beskrivelse av dette i noen av kontrollrapportene og dermed blir det vanskelig å slå fast hvorvidt personopplysninger er nødvendig eller ikke for å oppfylle formålet. Ut fra vanlig språkforståelse har jeg kommet frem til noen mulige svar på hva dette formålet kan innebære:

- Å lage statistikk
- Å lage grupperinger av kunder
- Å ta betaling/gi produkter det er betalt for
- Å behandle kundeservicehenvendelser.
- Å kartlegge reisemønster
- Å sende informasjon til kunder

Det meste av dette dekkes av de andre formålene kollektivtransportselskapene har opplyst over.

Unntaket er dersom administrering av kundemassen innebærer å sortere kundene i kategorier og/eller sende dem tilbud basert på deres personlige reisemønster eller preferanser. Dette ville i så fall bety at det er opprettet personprofiler og innebære en spesiell informasjonsplikt i henhold til popplyl § 21. En slik tolkning av formålet vil utvilsomt kreve innsamling av personopplysninger, men vil neppe kunne hjemles i noen av nødvendighetsgrunnene. Dersom kunden selv ønsker tilbud basert på profilering av seg selv kan det muligens ses på som "å oppfylle en avtale med den registrerte [...]".<sup>123</sup> Da vil imidlertid en slik avtale måtte inngås eksplisitt og det vil trolig være like enkelt å hente inn samtykke.

---

<sup>123</sup> Jfr. popplyl § 8 bokstav a.

### 3.4.2 Formålene som ikke krever behandling av personopplysninger

Jeg vil nå gå gjennom formålene som etter mitt skjønn ikke krever behandling av personopplysninger. Ettersom de følgende formålene ikke trenger behandling av personopplysninger blir det kun en rask gjennomgang for å begrunne dette. Etter denne gjennomgangen vil jeg se på de øvrige formålene og hvorvidt noen av disse kan bruke nødvendighetsgrunnene som behandlingsgrunnlag.

Å etablere statistikk til bruk ved planlegging av rutetilbud er fullt mulig å gjennomføre uten å identifisere kortets eier. De fleste løsninger i dag har en eller annen form for serienummer på kortet. Det er med andre ord ikke bare teknisk mulig å få mengdetall på antall reiser hos kundene, men også kartlegge reisemønstre uten å identifisere annet enn selve kortet. Det er også mulig å kompensere for ufullstendig statistikk ved tilleggstiltak som spørreundersøkelser eller telling av passasjerer.<sup>124</sup>

Å gi kunden refusjon i forbindelse med ubenyttet kort er et mindre selvsagt tilfelle enn de vi hittil har vært gjennom. Dersom en ubenyttet billett skal refunderes uten personlig oppmøte, vil dette kreve at billettens eier kan identifiseres og trolig at dette eierskapet er lagret, enten i en sentral database eller på selve kortet. Det er imidlertid mulig å gjennomføre refusjonsordninger som innebærer oppmøte uten å lagre personopplysninger.<sup>125</sup> En slik henvendelse vil være tilsvarende den beskrevet i Scenario 1.<sup>126</sup> Behovet for personopplysninger knyttet til kortet oppstår først om man ønsker å gjøre refusjonen lettere tilgjengelig. Der er i liten grad knyttet til nødvendighet, men snarere knyttet til tilgjengelighet, enkelhet og grad av kundeservice. Dersom kunden ønsker enklere tilgang til tilbudet, er det neppe noe som hindrer henne i å samtykke til behandling av personopplysninger gjennom å registrere kortet sitt.

Avregning mellom selskaper. Dersom det elektroniske billettsystemet et samarbeid mellom to kollektivselskaper, er det behov for å beregne fordeling av billettinntekter fra billetter som kan brukes i begge selskapene. Som jeg allerede har vært inne på er det mulig å etablere statistikk, også av typen som følger et korts bruksmønster, uten å lagre personopplysninger. Disse avregningene har også blitt gjort før elektroniske billetter var tatt i bruk.<sup>127</sup> Dermed er det liten tvil om at dette er mulig å gjennomføre uten bruk av personopplysninger.

Å kontrollere bruken av kortet betyr mest sannsynlig en av to ting. En mulighet er knyttet til billettkontroll, for eksempel å sjekke at en voksen ikke benytter seg av honnørbillett.<sup>128</sup> Det kan også handle om å følge bruksmønstre. Sistnevnte har jeg

---

<sup>124</sup> Begge disse metodene la grunnlaget for statistikken før de elektroniske løsningene var på plass.

<sup>125</sup> I mitt intervju med Helge Olsen Bye i Hedmark Trafikk, forklarte han at de gir refusjon til ihendehaver mot kvittering på kjøpt billett.

<sup>126</sup> Se kapittel 3.2.3.

<sup>127</sup> Tidligere ble avregning mellom Oslo Sporveier og Stor-Oslo Lokaltrafikk gjort ved å telle passasjerer som gikk av og på for eksempel T-banen kombinert med spørreundersøkelser av passasjerer.

<sup>128</sup> Mer om billettkontroll i kapittel 3.4.4.

tatt for meg i punktet å etablere statistikk. Det er kanskje mulig å se for seg at kollektivselskapet ønsker å kontrollere at en personlig billett kun brukes av eieren. Dette vil i tilfelle være dekket av et annet formål jeg skal komme tilbake til senere og derfor legger jeg ikke dette til grunn her.<sup>129</sup>

Feilsøking i datasystemet er også et relativt generelt formulert formål. Jeg antar at dette dreier seg om å lokalisere feil der deler av systemet ikke fungerer som det skal. For eksempel at turen ikke belastes kortet, eller kunden ikke får billetten hun har betalt for. I de tilfeller der feilen blir til ugunst for kunden, må man anta at kunden henvender seg med en klage, og på den måten oppretter nødvendig kontakt mellom behandlingsansvarlig og kortet. I andre tilfeller vil ofte kortnummeret være tilstrekkelig. Kortnummeret vil ofte kunne si noe om kortet er nytt eller gammelt og dermed også avdekke om feilen er knyttet til en versjon av programmeringen på kortene. Dette vil gjøre det mulig for behandlingsansvarlig å fremprovosere feilen i kontrollerte tester. Det er neppe noe problem for behandlingsansvarlig å skru av et defekt/feilfungerende kort gjennom en form for fjernstyring uten å vite annet en kortets nummer.

### 3.4.3 Formålene som krever behandling av personopplysninger

Jeg vil nå ta for meg de av formålene som krever en eller annen form for behandling av personopplysninger. Hvert punkt vil her ha en vurdering av hvorvidt noen av nødvendighetsgrunnene kan brukes som grunnlag denne behandlingen.

Å kontrollere at periodebilletten kun benyttes av en person krever en eller annen form for behandling av personopplysninger under selve kontrollen. Det er ikke dermed sagt at denne informasjonen må være lagret sentralt i billettssystemet eller i elektronisk format. Før elektroniske billettssystemer ble tatt i bruk, var det flere typer billetter som hadde fotografi, navn og egen identifikator på et slags "identitetskort" som ble knyttet til periodebilletten. Eksempler på slike løsninger er Ruters gamle (ikke-elektroniske) studentmånedskort eller SLs Ungdomskort<sup>130</sup>. I Bransjenormen omtales en slik løsning, med bilde på kortet uten sentral lagring som knytter identitet til kortnummer, som "tilstrekkelig anonymt"<sup>131</sup> til at det ikke regnes som behandling av personopplysninger.<sup>132</sup> Bransjenormen debatterer eller begrunner ikke dette i noen særlig grad. Som et minimum må det nok altså behandles opplysninger ved selve kontrollen av billetten. Et slikt tilfelle vil enten tilsvare Scenario 1, eller være en del av billettkontroll.<sup>133</sup>

Det kan tenkes at en personlig periodebillett har en lavere pris enn en tilsvarende upersonlig billett som kan brukes av flere. En slik situasjon ville nok kunne ses på

---

<sup>129</sup> Se formålene: "Å kontrollere at periodebilletten kun benyttes av en person" og "Å kontrollere at periodebilletten kun benyttes av rett person" i kapittel 3.4.3.

<sup>130</sup> Ungdomskortet var en periodebillett for ungdom mellom 16-20 år.

<sup>131</sup> Bransjenormen, s. 3.

<sup>132</sup> Mer om Bransjenormen i kapittel 6.

<sup>133</sup> Mer om billettkontroll i kapittel 3.4.4.

som at det oppfylles en avtale, jamfør popplyl § 8 bokstav a. Behandlingen av personopplysninger er ikke nødvendig for å gi kunden den delen av avtalen hun har krav på. Den er et tilleggsvilkår den behandlingsansvarlige selv har definert som en del av avtalen. Lovens forarbeider bruker en ordlyd som ser ut til å understreke behovet for at den registrerte skal ta initiativ til avtalen som setter i gang behandlingen, samt at behandlingen skal være nødvendig for å kunne gi tilbudet.<sup>134</sup> Sistnevnte ser ikke ut til å være oppfylt her. Lovens § 8 bokstav a er i en særstilling blant nødvendighetsgrunnene fordi enhver form for avtaleinngåelse vil inneholde et element av samtykke i seg. Dermed er det vanskelig å se for seg en situasjon der en slik behandling kan hjemles gjennom samtykke. Trolig vil bokstav a uansett ikke kunne begrunne krav til at kortet skal være registrert, kun behandling av personopplysninger som oppstår ved kontroll av billetten.

Til slutt må dette formålet vurderes i lys av bokstav f. Denne siste nødvendighetsgrunnen er den mest generelt formulerte og dermed den som krever mest omfattende debatt av de 6. Selv om den kan virke åpen, er den også den eneste av nødvendighetsgrunnene som eksplisitt krever en avveining for å tas i bruk. Interessen til den behandlingsansvarlige (eller tredjeperson) må overstige hensynet til den registrertes personvern, Dette handler delvis om å sikre at kundene løser korrekt billett og dermed betaler for driften av kollektivtilbudet. Det er altså forbundet med kollektivselskapets interesse i å få inntekter. Det er imidlertid ikke slik at inntektsgrunnlaget deres står og faller på denne muligheten til å behandle personopplysninger da det som nevnt finnes anonyme alternativer. I sak nr. 2004/3 påpeker Personvernemnda at i henhold til forarbeidene skal «hensynet til privatlivets fred [...] tillegges betydelig vekt i avveiningen mot kommersielle interesser.»<sup>135</sup>. Hvorvidt dette betyr at kommersielle interesser er mindre viktige enn andre interesser, eller kun får "lavstatus" når de kommer i konflikt med privatlivets fred, er vanskelig å si. Privatlivets fred må nok grovt sett begrenses til hjemmet og kommunikasjon<sup>136</sup>. Personverndirektivets tilsvarende bokstav f er formulert noe annerledes og henviser til hensynene i formålsparagrafen. I direktivets formålsparagraf står det at formålet er å: "sikre vern av fysiske personers grunnleggende rettigheter og friheter, særlig retten til privatlivets fred, ved behandling av personopplysninger". Dersom man anser retten til å ferdes anonymt som en grunnleggende rettighet eller frihet, vil dette tale for å vekte personvernens hensyn i denne saken. Bruken av kollektivtransport er såpass omfattende i deler av landet og noe en stor del av befolkningen er avhengig å bruke daglig. Det blir derfor ikke et reelt alternativ å velge bort kollektivt dersom man ønsker å reise anonymt. I PVN-2005-11 går Personvernemnda langt i å kalle anonym ferdsel en grunnleggende

---

<sup>134</sup> Ot.prp. nr 92 (1998-99), Kapittel 16.

<sup>135</sup> Ot.prp. nr 92 (1998-99), side 109.

<sup>136</sup> Telefon, brev, e-post, samtaler og andre tilfeller der det er naturlig å være privat.

rettighet.<sup>137</sup> Ettersom anonyme likeverdige løsninger er gjennomførbart, er det naturlig å anta at slike løsninger må tas i bruk.

Bokstav f kan dermed neppe begrunne krav til registrerte kort i slike tilfeller, men kan muligens begrunne behandlingen som oppstår ved kontroll av billetten.

Å kontrollere at periodebilletten kun benyttes av rett person dreier seg om mye av det samme som forrige formål. Dersom rett person i dette tilfellet er kortets eier, vil disse formålene i praksis gå ut på det samme. En rett person kan også være det samme som en person som har krav på en viss type billett. Da vil vurderingene bli de samme som i diskusjonen om moderasjonsbevis under formålet "å få bekreftet at kunden har en gyldig billett".

Å få bekreftet at kunden har gyldig billett vil hovedsakelig være aktuelt ved påstigning eller billettkontroll.<sup>138</sup> I de tilfeller der vedkommende mottar en eller annen form for rabatt vil det være behov for ytterligere informasjon om kunden. Dette vil som regel kunne løses ved fremvisning av moderasjonsbevis.<sup>139</sup> Moderasjonsbeviset vil som regel inneholde tilstrekkelige personopplysninger i form av bilde eller navn. Det er altså ikke noe behov for å lagre disse opplysningene hos behandlingsansvarlig for å bekrefte at billetten er gyldig. Det er tilstrekkelig å lagre hva slags type billett kortet inneholder.

Å belaste kundens reisekonto kan også bety to ting. Enten er en reisekonto en slags virtuell verdi knyttet til billetten. Beløper eller enheter kan trekkes fra billetten hver gang den brukes uten at kortet registreres.

Den andre muligheten er at det er snakk om en abonnementstjeneste med automatisk trekk fra kundens konto. For eksempel såkalt A-kort<sup>140</sup>. Dette er et formål som er avhengig av gyldig betalingsinformasjon og som av sikkerhetshensyn vil kreve behandling av personopplysninger. Dersom en kunde ønsker å benytte seg av et slikt tilbud, vil dette kreve registrering av kortet. En slik løsning vil nok kunne hjemles i popplyl § 8 bokstav a, "å oppfylle en avtale med den registrerte". Dersom tjenesten innfris før konto belastes vil en eventuell innkrevingsprosess<sup>141</sup> kreve behandling av personopplysninger som trolig kan kalles en "berettiget interesse" etter bokstav f. Forutsetningen her er at kunden selv har tatt initiativet og bestilt tjenesten.

Rekonstruksjon av tapte kort forutsetter kunnskap om hva kortet inneholdt og muligheten til å bekrefte at vedkommende som mottar nytt kort også er eier av det gamle. Sistnevnte for å kunne forhindre at eksisterende kunder ved en feil, eller som

---

<sup>137</sup> "Personvernemnda slutter seg fullt ut til Datatilsynets oppfatning av at spørsmålet om retten til å ferdes anonymt på offentlig sted, og ellers til å opptre anonymt i samfunnet, er et grunnleggende rettspolitisk spørsmål av sentral betydning for personvernet."

<sup>138</sup> For mer utfyllende om billettkontroll, se kapittel 3.4.4.

<sup>139</sup> For eksempel gyldig studentbevis.

<sup>140</sup> A-kort er et månedskort/periodebillett som tidligere kom hjem til deg i posten, men som i elektronisk form kan fornyes ved en oppdatering i datasystemet.

<sup>141</sup> For eksempel hvis transaksjonen ikke kan gjennomføres av manglende dekning eller lignende.

resultat av svindel, skal få gyldige kort sperret. I intervjuer med casene mine har denne muligheten blitt framhevet som en tilleggsteneste og et sentralt argument for å registrere kortet sitt. Det er rimelig at dette tilbudet skal forutsette registrering da manglende sikkerhet vil kunne åpne for svindler som potensielt kan koste kollektivselskapene og de registrerte store summer. Samtidig er mitt inntrykk at dette er et såkalt "selling point" ovenfor kunder som vurderer å registrere seg. Kundene vil dermed kanskje velge å registrere seg nettopp for å få dette gode, eller i det minste under forutsetningen av at det er tilgjengelig. Slikt sett faller denne behandlingen under bokstav a, men vil trolig allerede være resultatet av et samtykke. Behovet for å behandle personopplysninger er en forutsetning for at kollektivselskapet skal kunne gi kunden et tilbud som koster selskapet penger og slikt sett er til selskapets ugunst.<sup>142</sup> Utover dette har personopplysningene kun en interesse for kollektivselskapet i den grad opplysningene i seg selv er verdifulle. Dette kan neppe sies å være en tilstrekkelig berettiget interesse etter bokstav f.

Håndtering av kunder/bedre kundeservice. Dersom en kunde henvender seg med en klage, må det selvsagt behandles personopplysninger til saken er løst. I saker som ikke kan løses der og da, men krever oppfølging på et senere tidspunkt, må opplysningene lagres i en gitt periode. En slik form for behandling krever imidlertid ikke at navnet er knyttet til billetten på forhånd. Kundesenteret kan for eksempel åpne en sak i kundens navn der all relevant informasjon er lagret og slette disse opplysningene en viss tid etter at saken er avsluttet. Som jeg har vært inne på tidligere, vil kollektivselskapet trolig kunne tilby flere og bedre tjenester til en kunde med registrert kort. Det vil neppe være til stor ugunst for den behandlingsansvarlige å ikke kunne tilby disse tjenestene. Slike tjenester preg av å være tilleggstenester kunden kan velge å benytte seg av. Det er neppe grunnlag for å hevde nødvendighet i noen av disse situasjonene. Selv om det er i kundenes interesse, vil det ikke tilfredsstillende kravet om "allmenn interesse" etter bokstav d. Allmenn må nok tolkes mer i retning av samfunnsinteresse enn "praktisk for mange". Det kan også tenkes at "å håndtere kundene" er knyttet til trafikkbildet og dermed er beslektet med "å etablere statistikk til bruk ved planlegging av rutetilbud". Som jeg har nevnt er dette mulig å gjennomføre uten innsamling av personopplysninger. Dermed er dette neppe nødvendig eller en berettiget interesse å tilrettelegge tilbudet til kundene basert på dataene som er samlet inn. Også selv om det fører til økt omsetning.<sup>143</sup>

Fakturering av abonnementstjenester. Se diskusjonen om "å belaste kundens reisekonto" over.

Så vidt jeg kan se, vil enkelte av nødvendighetsgrunnene kunne benyttes i noen få av disse formålene. Flere av disse formålene bærer preg av å være tilbud til kunden

---

<sup>142</sup> Alternativet er at kunden må kjøpe nytt kort.

<sup>143</sup> OsloTrikken har for eksempel erfaringer med at "Rullende Fortau" – en endring i kjøremønster førte til reduserte kostnader og flere passasjerer: Oslotrikken, *Årsrapport Oslo Sporvognsdrift AS 2006 (2007)*, s.4.

og således er det ingenting i veien for at avtaleinngåelsen innebærer innhenting av samtykke fra de som ønsker dette tilbudet. Slik jeg ser det er det neppe mulig å bruke nødvendighetsgrunnene til å begrunne registrering av kort, men i enkelte tilfeller kan de brukes til å begrunne behandling av personopplysninger i konkrete situasjoner, som for eksempel refusjon av billett eller kontroll av moderasjonsbevis.

#### 3.4.4 Billettkontroll

Billettkontrollen befinner seg i en særstilling i forhold til de andre formålene. Med billettkontroll menes uanmeldte billettkontroller med det formål å avsløre reisende uten gyldig billett, samt forebygge at folk reiser uten gyldig billett. Dersom noen blir kontrollert uten gyldig billett, blir vedkommende som regel bøtelagt. Min drøftelse har tatt utgangspunkt i hvorvidt det er nødvendig med kundens navn knyttet til billetten eller ikke. Jeg kan imidlertid ikke utelukke at formålet ”å kontrollere at kunden har gyldig billett” er ment for å dekke behandlingen av personopplysninger som oppstår når en kunde med uregistrert billett blir tatt i billettkontroll. I tillegg til koblingen mellom kundens ansikt og den ugyldige billetten,<sup>144</sup> vil det også bli behandlet personopplysninger i forbindelse med fakturering og innkreving av tilleggsavgift. Drøftelsene i kapittelet over har ikke tatt for seg disse perspektivene. Billettkontrollen er sporadisk og kan klassifiseres som et tilleggs- eller ekstratiltak utover vanlig drift. Disse formene for behandling av personopplysninger vil bare unntaksvis kreve lagring av opplysningene.<sup>145</sup> Som nevnt er det mulig å kontrollere billett uten at kortet er registrert. Det er imidlertid liten tvil om at kollektivselskapet har en ”berettiget interesse” i å hindre at kundene ikke betaler for seg. Dersom formålet er å gjennomføre billettkontroll vil krav til bruk av samtykke være til hinder for at formålet med behandlingen kan gjennomføres. Kredittnett AS har tatt opp en sak for Personvernemnda der nemnda peker på hvordan det å kreve samtykke kan gå på bekostning av opplysningenes kvalitet.<sup>146</sup> Billettkontrollens behandling av personopplysninger bør dermed heller hjemles i popplyl § 8 f. Forutsatt at det er snakk om behandling som oppstår når billetter kobles til eieren gjennom møte med kontrollør og bruk av navn og adresse i fakturerings- eller innkreivingsøyemed.<sup>147</sup>

#### 3.4.5 Skoleskyssordningen

Skoleskyssordningen er en tjeneste som tilbys av kollektivtransportfirmaer over hele landet på vegne av det offentlige. Ordningen er hjemlet i opplæringslovas kapittel 7. I den grad behandling av personopplysninger er en forutsetning for å kunne tilby Skoleskyss kan det sies å være en implisitt lovhjemmel for behandlinger i opplæringslova. Skoleelever har krav på betalt skyss dersom skoleveien deres er lang eller spesielt vanskelig<sup>148</sup>, eller dersom spesielle helseforhold tilsier dette.

---

<sup>144</sup> Ref. drøftelsene i kapittel 3.2.3 og 3.2.4.

<sup>145</sup> Dersom kunden har gyldig billett eller tilleggsavgiften betales på stedet, er det ikke behov for videre lagring.

<sup>146</sup> KLAGESAK 2003/01: Klage på Datatilsynets vedtak i sak om avslag på konsesjonssøknad for opprettelse av sentralt lånerregister.

<sup>147</sup> Opplysningene skal selvsagt slettes i det de ikke lenger er nødvendige, jmfør popplyl § 28.

<sup>148</sup> For eksempel dersom de er avhengige av båt eller skoleveien er farlig å ferdes til fots.

Skoleskyss er en tjeneste som tilbydere av kollektivtransport plikter å tilby.<sup>149</sup> Det er en rekke kriterier som må være tilfredsstillende for at en elev skal ha krav på et slikt kort. At vedkommende er registrert som elev i rett klassetrinn og at det er gjort en vurdering av hvorvidt elevens skolevei tilfredsstiller kravene i opplæringslova er noen av dem. Dette er forhold det er umulig for kollektivselskapet å vurdere fra gang til gang, men som nødvendigvis vil være avgjort på forhånd. Enkelte av begrunnelser for rett til skoleskyss vil kunne være helseopplysninger<sup>150</sup>, og sånn sett er det heller ikke tilrådelig at kollektivselskapet besitter vurderingsgrunnlaget.

Det mest hensiktsmessige er at kollektivselskapet ved opprettelse av skoleskysskort får opplysningene de trenger for å opprette kortet for så å kvitte seg med disse når kortet er produsert. Slike opplysninger vil for eksempel være personalia, bilde og en bekreftelse på at eleven er innvilget skoleskyss. Behovet for å bekrefte at rett person bruker rett kort vil her kreve behandling av personopplysninger fordi det ikke eksisterer noe moderasjonsbevis som kan bekrefte elevens krav på ordningen. Dette skiller seg fra andre tilleggstjenester kollektivselskapet tilbyr ved at det er en rettighet eleven har.

Det er en klar lovhjemmel for å bruke disse opplysningene. Samtidig er dette en rettighet man søker om, og slikt sett kan det sies å være samtykke knyttet til behandlingsgrunnlaget. Skoleskyssordningen kan nok også muligens begrunnes i popplyl § 8 bokstav d som en oppgave av allmenn interesse. Ordningen gjelder nok et klart mindretall av de reisende og er ikke en del av det generelle publikumstilbudet. Det er derfor lite interessant å utdype dette videre i oppgaven og jeg vil nøye meg med å konstatere at behandling av personopplysninger i en eller annen form blir nødvendig samt at det ser ut til å være opptil flere mulige behandlingsgrunnlag.

### 3.5 Rettslige krav til samtykke

I kapittel 3.3 viser jeg at samtykke alltid har forrang i den grad det er mulig å benytte seg av det. Med unntak av tilfellet billettkontroll og Skoleskyss skal samtykke være et mulig behandlingsgrunnlag i de fleste tilfellene jeg har vært innom. Videre ser vi av kapittel 3.4 at det i de aller fleste tilfeller er lite aktuelt å benytte seg av noen av nødvendighetsgrunnene i popplyl § 8 a-f som behandlingsgrunnlag. Det er enkelte tilleggstjenester som krever behandling av personopplysninger, men disse er enten ikke-essensielle for drift eller gjennomførbare uten personopplysninger som genereres ved bruk av kortet. Dermed gjenstår samtykke som eneste måten å begrunne behandling av personopplysninger som følger av bruk av registrerte kort. Registreringen av kortet må med andre ord være basert på et samtykke.

---

<sup>149</sup> Plikten er indirekte ved at den for eksempel er en forutsetning i en anbudskonkurranse. Dersom selskapet eies av det offentlige, vil det ofte være eneste tilgjengelige "verktøy" for å ha tilstrekkelig tilbud.

<sup>150</sup> For eksempel etter opplæringslova § 7-3. Slike opplysninger er sensitive personopplysninger etter popplyl § 2 nr 8.



Selv om det juridiske begrepet "samtykke" er forklart med egen legaldefinisjon i popplyl § 2 nr.7, inneholder selve legaldefinisjonen vage termer. Schartum skriver i norsk lovkommentar at det ikke stilles formkrav til samtykket i personopplysningsloven.<sup>151</sup> I § 2 nr. 7 defineres samtykke som "en frivillig, uttrykkelig og informert erklæring fra den registrerte [...]" og dette er tradisjonelt sett tolket i streng forstand.<sup>152</sup> Det er altså ingen konkrete krav til hvorvidt samtykket kan gis via en nettside eller på fysisk papir, om det kan gis muntlig eller skriftlig. Loven stiller først og fremst krav til konteksten for samtykket, inkludert konsekvensene ved å nekte og informasjonsplikten til den behandlingsansvarlige.

Selv om det ikke stilles formkrav til samtykkeerklæringen, er det mulig å se for seg situasjoner der samtykket bør dokumenteres. For eksempel dersom det er strid om avtalens innhold. I popplyl § 14 stilles det krav til rutiner for internkontroll. Disse rutinene skal omhandle alle krav loven stiller, herunder rutiner for hvordan den registrerte informeres etter informasjonsplikten i § 19. Alle rutinene skal kunne dokumenteres. Å dokumentere om og hvordan en eventuell muntlig informasjon i forkant av et samtykke skal gis, vil være svært omfattende. Det er derfor nærliggende å tro at behandlingsansvarlig i praksis ofte blir nødt til å samle inn samtykke på en måte som forutsetter en eller annen grad av skriftlighet. Enten ved at samtykkeerklæringen i seg selv er skriftlig, eller ved at det finnes nedfelt en form for skriftlig instruks om hva det informeres om og hvordan.

Antagelig vil en løsning som innebærer skriftlig samtykke ofte være mest hensiktsmessig for den behandlingsansvarlige. Dette vil gi god intern oversikt over blant annet formålet med behandlingen i tillegg til dokumentasjon i eventuelle stridsspørsmål. Det er imidlertid enkelt å se for seg situasjoner der skriftlig samtykke kan oppleves som unødvendig byråkratisk, tungvint og kostbart. Skriftlighet kan nok ikke anses som et absolutt krav.

I tillegg til kravene som følger av selve samtykkedefinisjonen, er det også en rekke krav som følger av personopplysningsloven for øvrig. Jeg har vært inne på disse tidligere, men vil forsøke å konkretisere disse i kapittel 3.6. Først vil jeg se nærmere på hva som ligger i de tre kjernebegrepene "frivillig", "informert" og "uttrykkelig". Deretter vil jeg forsøke å konkretisere dette ytterligere sammen med de øvrige kravene i personopplysningsloven.<sup>153</sup> Her vil fokuset være mer spesifikt på elektroniske billettsystemer og prosessen med å registrere<sup>154</sup> kortet.

I denne oppgaven begrenser jeg meg til å se på selve innsamlingen av personopplysninger og informasjonen som gis til den registrerte. Oppgaven legger ikke opp til en omfattende undersøkelse av casenes interne rutiner og således er det

---

<sup>151</sup> Schartum, Dag Wiese (2008), *Norsk lovkommentar: personopplysningsloven*, note14.

<sup>152</sup> Se for eksempel KLAGESAK 2003/01 og KLAGESAK 2005-06: *Klage på vedtak om pålegg i forbindelse med tilsyn hos Securitas, samt begjæring om at deler av vedtaket gis oppsettende virkning.*

<sup>153</sup> Se kapittel 3.6 flg.

<sup>154</sup> Altså knytte sin egen identitet til kortet/billetten.

naturlig at jeg primært ser på de krav som kan måles på "overflaten" av systemet. Målet er å ende opp med en konkret liste med krav som jeg kan bruke som vurderingsgrunnlag ovenfor casene i kapittel 4 og 5.

### 3.5.1 "Frivillig"

Enhver form for samtykke vil være en aktiv handling, og dermed kan kravet til frivillighet fremstå som noe selvsagt eller overflødig. For at frivilligheten skal være reell er det imidlertid en rekke ting som må på plass. Det kan for eksempel tenkes at et manglende samtykke vil gi en eller annen form for negativ konsekvens eller manglende tilgang på et gode. Som hovedregel vil dette gi en utfordring til frivilligheten i samtykket.

I forarbeidene til personopplysningsloven, presiseres det at "I kravet til at samtykket skal være frivillig ligger at det ikke må være avgitt under noen form for tvang fra den behandlingsansvarlige eller andre."<sup>155</sup> (min understreking). Dette innebærer at det å ikke gi sitt samtykke ikke kan få negative konsekvenser eller gi særlig stor ulempe. Jeg vil trekke frem to saker fra Personvernnemnda som bidrar til å trekke grensene for reell frivillighet i forbindelse med samtykke.

Personvernnemndas klagesak fra Securitas<sup>156</sup> omhandler arbeidsgivers mulighet til å rusmiddelteste ansatte basert på samtykke. Arbeidsgiveren påpeker i den aktuelle saken at ettersom det bes om samtykke til rusmiddeltesting etter ansettelse, vil dette ikke påvirke selve ansettelsesprosessen. Videre anfører arbeidsgiver at eventuell nekting ikke vil få følger for den ansattes arbeidssituasjon. Til tross for dette peker nemnda på at det alltid vil være et skjevt maktforhold mellom arbeidsgiver og arbeidstaker og at dette bidrar til at frivilligheten i et slikt samtykke ikke er reell.

I Personvernnemndas sak om dopingtester ved Skullerud Sport Senter AS,<sup>157</sup> peker nemnda på et mulig stort sosialt press, men lander på at frivilligheten i samtykket fortsatt er reell. Denne saken skiller seg fra saken om rusmiddeltesting på arbeidsplassen ved at maktperspektivet mellom arbeidstaker og arbeidsgiver ikke er til stede. I tillegg vil de som mottar samtykke fra brukerne av treningssenteret i langt mindre grad være i stand til å skaffe seg oversikt over alle treningssenterets brukere. Dermed vil det være reell anonymitet for de som velger ikke å samtykke. Disse to momentene taler for at potensialet for sosialt press ikke kan tillegges vekt i den grad at det ugyldiggjør samtykket i denne konkrete saken.

I Norsk Lovkommentar til personopplysningsloven er Dag Wiese Schartum inne på muligheten for det han kaller strukturell tvang.<sup>158</sup> Eksempelet han bruker er en tenkt situasjon der alle forsikringsselskap krever installert GPS som betingelse for å få

---

<sup>155</sup> Ot. Prp. nr. 92 (1998-99), Kapittel 16.

<sup>156</sup> KLAGESAK 2005-06 (Securitas)

<sup>157</sup> PVN-2006-06: *Dopingprøver. Klage på Datatilsynets vedtak om at dopingtester ved treningssenteret Skullerud Sport Senter AS skal opphøre.*

<sup>158</sup> Schartum (2008), note 13.

forsikring. Forsikringen er nødvendig for å få lov å kjøre bilen, og konsekvensene ved å ønske ikke få sine bevegelser loggført er dermed såpass store at de ikke kan anses som reell frivillighet. Schartum hevder det skal svært mye til før man eventuelt skal kunne hevde at slik strukturell tvang foreligger.

### 3.5.2 "Informert"

Et informert samtykke er et samtykke der den registrerte blir introdusert for all relevant informasjon i forkant av samtykkeerklæringen. Popplyl § 19 gir informasjonsplikt til den behandlingsansvarlige dersom opplysningene samles inn fra den registrerte selv. Å samle inn opplysninger generert gjennom bruk av en personlig billett må anses som å samle inn opplysninger fra den registrerte. Informasjonsplikten etter § 19 gjelder uavhengig av om behandlingen av personopplysninger er basert på samtykke eller ikke og uavhengig om den registrerte ber om informasjonen. Schartum skriver i lovkommentaren at punktene nevnt i § 19 a-d er et minimum:<sup>159</sup>

*"Om:*

- a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,*
- b) formålet med behandlingen,*
- c) opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,*
- d) det er frivillig å gi fra seg opplysningene, og*
- e) annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28."*

Som tidligere nevnt, er det ingen formkrav til hvordan denne informasjonen presenteres, kun at innholdet presenteres på en slik måte at det er tydelig for den registrerte. Ettersom den behandlingsansvarlige plikter å gi informasjon om "annet som gjør den registrerte i stand til å bruke sine rettigheter [...] på best mulig måte"<sup>160</sup> bør det gjøres en vurdering basert på hva slags opplysninger som samles inn og formålet de samles inn for. Den registrertes interesse i å rette feilaktig informasjon vil for eksempel anses som mindre viktig/relevant i forbindelse med elektroniske billetter enn i en søknad om stønad. Informasjonen bør være strukturert på en slik måte at det mest relevante er tydeligst i den grad det lar seg gjøre. Dersom den registrerte har personlig kontakt med en representant for den behandlingsansvarlige, vil det kanskje være mulig å tilpasse informasjonen etter den enkeltes behov også, og ikke bare på generelt grunnlag. Trolig vil dette kravet kunne avvikes dersom kartleggingen av den registrertes behov innebærer behandling av ytterligere personopplysninger.

---

<sup>159</sup> Schartum (2008), note 15.

<sup>160</sup> Jfr. popplyl § 19 bokstav e.

For at samtykket skal være informert må det informeres tydelig i forkant om at en aksept er det samme som et samtykke og hva det samtykkes til. Dette gir et implisitt krav til fravær av tvetydighet. Den behandlingsansvarlige har et ansvar for at informasjonen som gis den registrerte ikke er unødvendig uklar eller enkelt kan misforstås. Den behandlingsansvarlige bør forsøke å unngå bransjespesifikke termer eller unødvendig avansert språk. Det kan oppstå situasjoner der negative konsekvenser for den registrertes personvern er en vanlig følge av å ikke samtykke, eller disse er spesielt godt kjent for den behandlingsansvarlige. I slike tilfeller bør en naturlig følge av popplyl § 19 bokstav e, være at dette må informeres om i forkant av samtykket.<sup>161</sup>

Antageligvis vil tydelighetskravet gi noen formkrav til informasjonen. Liten skrift nederst på en side, eller at teksten som gir nødvendig informasjon er gjemt i en lang ToS<sup>162</sup>, vil neppe kunne anses som tydelig nok.

Det er ikke uvanlig at personopplysninger byttes mot et gode. Typisk samtykker man dermed både til at opplysningene behandles for å kunne tilby nevnte gode og godkjenner bruk av personopplysninger som først og fremst er i behandlingsansvarliges interesse. Typiske eksempler er adresseinfo til reklameutsending eller forbrukerdata for statistiske formål. Dersom godet er overkommunisert i forhold til det andre formålet, vil dette kunne ha en villedende effekt på lik linje med liten skrift. Kanskje bør informasjon om mulige personvernkonsekvenser holdes tydelig adskilt fra informasjon om goder.

Lovens formål er å beskytte den registrerte, noe som taler for at store konsekvenser for den enkeltes personvern medfører strengere krav til informasjonen som gis.

### 3.5.3 "Uttrykkelig"

I tillegg til å være frivillig og informert, skal samtykket være en "uttrykkelig[...] erklæring fra den registrerte". Ofte vil erklæringen være forfattet på forhånd av behandlingsansvarlig og deretter signert eller på annen måte attestert av den registrerte. I forrige kapittel understreket jeg det av informasjonen som gis den registrerte må komme tydelig frem at det samtykkes og hva det samtykkes til. En slik tekst vil ofte henvise til informasjonen som nettopp ble gitt og dermed vil kravet til uttrykkelighet delvis overlappe kravet til at samtykket skal være "informert".<sup>163</sup>

Trolig vil kravet til uttrykkelighet også forutsette at samtykket er en aktiv handling. Som hovedregel vil gyldig samtykke neppe kunne anses hentet inn gjennom negativ aksept<sup>164</sup>. En forhåndsformulert samtykkeerklæring vil kunne være tilstrekkelig uttrykkelig om den "signeres" ved å krysse av i elektroniske bokser eller lignende. Å

---

<sup>161</sup> Schartum (2008), note 15.

<sup>162</sup> Forkortelse for "Terms of Service", en lengre liste vilkår man godtar for å få lov å bruke et produkt. Mest brukt i forbindelse med installering av software.

<sup>163</sup> Se kapittel 3.5.2 ovenfor.

<sup>164</sup> Altså at manglende respons blir ansett for å være en godkjennelse.

krysse av i en boks er en aktiv handling, men kanskje vil det å krysse av for å ha lest en rekke vilkår, hvorav et av dem er samtykke være beslektet med et passivt<sup>165</sup> samtykke. Som hovedregel er det antagelig slik at jo vanskeligere det er å forutse konsekvensene av samtykket og jo mindre aktiv samtykkesituasjonen er fra den registrertes side, jo strengere bør kravene være til informasjonens tydelighet.

Også her gjelder prinsippet om at jo større konsekvens for den registrertes personvern, jo strengere krav til samtykkeerklæringen.

### 3.6 Krav til gjennomføring av samtykke i praksis

Nå som jeg har drøftet mulige behandlingsgrunnlag og trukket opp noen generelle avgrensninger rundt samtykke, er det på tide å se enda mer spesifikt på elektroniske billettsystemer. Under har jeg laget en liste med krav som følger av personopplysningsloven generelt og samtykke spesielt. Enkelte av punktene har en noe generell karakter, og i løpet av de neste kapitlene skal jeg forsøke å konkretisere dette ytterligere. Jeg vil gjennomgå kravene se på hvilke konkrete følger de bør få for et kollektivselskap som samler inn personopplysninger gjennom sitt elektroniske billettsystem. Jeg vil fokusere på de krav som oppstår i forbindelse med valg av samtykke som behandlingsgrunnlag, innsamling av opplysningene samt de forpliktelser behandlingsansvarlig får direkte ovenfor den registrerte. Dette betyr at jeg ikke vil gå i detalj på programmeringsnivå, eller se nærmere på datasikkerheten. Hvilke muligheter den registrerte har til innsyn, er derimot noe jeg anser som relevant i forhold til spørsmålene i denne oppgaven. Dette fordi det handler om den registrertes opplevelse av at vilkårene for samtykket er oppfylt. Etter å ha konkretisert disse kravene vil jeg forsøke å oppsummere dette i en mer spesifikk liste over krav. Denne listen vil være utgangspunktet for vurderingen av casene i kapittel 4 og 5.

Den foreløpige listen med krav er som følger:

- Formål er formulert og begrunnet i bedriftens virksomhet.
- At innhenting av samtykke er gjennomførbart.
- At det finnes anonyme alternativer til registrert billett.
- Det lages en registreringsrutine som sikrer gyldig samtykke.
- Informasjonsplikten er overholdt.
- At det er tilrettelagt for innsyn for den registrerte.
- Melding om behandling av personopplysninger er sendt til Datatilsynet.
- Sletteplikten er overholdt.
- Den registrerte har tilgang på å rette mangelfulle opplysninger.
- Tilstrekkelig informasjonssikkerhet.
- Internkontroll.

Jeg vil gjennomgå kravene etter samme modell som jeg brukte under gjennomgangen av formålene i kapittel 3.4.2 og 3.4.3.

---

<sup>165</sup> Eller negativ aksept.

### 3.6.1 Nærmere om den foreløpige kravlisten

En grunnleggende forutsetning for å behandle personopplysninger er at formål er formulert og begrunnet i bedriftens virksomhet. Dette er også avgjørende for valg av behandlingsgrunnlag og er et krav etter popplyl § 11 bokstav b og c. Formålet skal sette grenser for hva personopplysningene kan brukes til og bør derfor ha en tydelig avgrensing. I enkelte tilfeller vil formålet være avgjørende for om behandlingen er regulert av, eller kan hjemles i, andre lover enn popplyl.

Det mest vesentlige for elektroniske billetter blir imidlertid at formålet er begrunnet i bedriftens virksomhet. Dette betyr at formålet ikke kan være hva som helst. For eksempel vil det neppe være mulig å begrunne et behov for å kartlegge identifiserbare enkeltpersoners geografiske plassering over tid i bedriftens virksomhet. Til gjengjeld er det trolig mulig å begrunne et behov for å se på reisemønstre som et ledd i å kartlegge anonymiserte kunders adferd. Disse to formålene vil i stor grad innebære lagring av de samme reisedataene. Forskjellen består i hvordan man velger å sammenstille opplysningene og i hvilken grad de anonymiseres i ettertid. Formålet må altså antagelig begrenses til å bidra til effektiv drift av kollektivtransport og tilbud til kundene.

Det er viktig å understreke at dersom innhenting av samtykke er gjennomførbart, blir det også avgjørende for valg av behandlingsgrunnlag.<sup>166</sup> Dette vil ikke bare innebære at en erklæring kan innhentes fra kundene, men også forutsette at det er mulig å gi dem tilstrekkelig informasjon slik at samtykket er gyldig. Trolig kan ikke erklæringen være passiv, men må innhentes på en slik måte at det gis en selvstendig samtykkeerklæring. Det er ingenting i veien for å legge samtykket inn i kjøpsprosessen, men en negativ aksept knyttet til kjøpet, er trolig ikke godt nok. Alternativt kan man legge til rette for å registrere anonyme billetter på et senere tidspunkt og dermed samtykke i ettertid.

At det finnes anonyme alternativer til registrert billett er en forutsetning for at frivillighetskravet til samtykket skal anses som reelt og sånn sett beslektet med forrige punkt. Det er nok en viss overlapp med kravet "Lage registreringsrutine som sikrer gyldig samtykke" ettersom frivillighetskravet nødvendigvis blir en del av et gyldig samtykke. Jeg har valgt å nevne dette som et selvstendig punkt, fordi det er nødvendig for kollektivselskapet å vite at de har denne tekniske muligheten for å kunne velge samtykke som behandlingsgrunnlag. Ofte vil billettsystemer som er utviklet med registrerte billetter som utgangspunkt ha problemer med å tilby et anonymt alternativ.<sup>167</sup> Det kan bli kostbart å programmere om et system i ettertid og i enkelte tilfeller vil det ikke la seg gjøre uten å bygge nytt system.

Uavhengig av hvilket behandlingsgrunnlag som skal brukes må melding om behandling av personopplysninger sendes til Datatilsynet. Kravet om melding følger

---

<sup>166</sup> Ref. drøftelsen i kapittel 3.3.

<sup>167</sup> Ifølge Bjørn Rune Holmen ble systemet bak Innlandskortet programmert med registrerte kort som utgangspunktet. Brorparten av personopplysningene som ble lagret var et resultat av dette.

av popplyl § 31. Det er imidlertid formulert en del unntak for meldeplikten i personopplysningsforskriften jamfør popplyl § 31 siste ledd. Pof § 7-12 gir den behandlingsansvarlige mulighet til å opprette et personvernombud istedenfor. I pof § 7-7 er det unntak fra meldeplikten dersom behandlingen gjelder "kunder, abonnenter og leverandører" og kun dersom "personopplysningene behandles som ledd i administrasjon og gjennomføring av kontraktsforpliktelser".

Hvorvidt samtykket er en del av en avtale som kan regnes som en kontraktsforpliktelse er jeg usikker på. Alle definisjoner jeg har sett refererer til kontrakter som rettslig bindende avtaler. Dette vil nok forutsette at brudd på kontrakten gir rettslige konsekvenser. Ofte vil kunden lokkes med tilbud om tilleggstjenester som automatisk fornyede månedskort eller rekonstruksjon av tapte kort i bytte mot samtykke. Dersom dette ikke innfris vil det muligens være brudd på forbrukerkjøpsloven og således kunne få en rettslig konsekvens for kollektivselskapet. Dette forutsetter løfte om gjenytelse fra behandlingsansvarlig. I de tilfeller der det blir bedt om samtykke uten at løfte om tilleggstjenester eller økonomisk kompensasjon gis vil imidlertid ikke dette unntaket fra meldeplikten gjelde.

For at unntaket skal være gjeldende, vil det trolig forutsette at opplysningene utelukkende brukes til å administrere og gjennomføre kontraktsforpliktelser. Dersom formålet med behandlingen innebærer å kartlegge bruksmønster hos kunder eller regne ut fordeling av inntekter mellom to selskaper vil meldeplikten være til stede.

Videre kan jeg vanskelig se for meg en situasjon der kollektivselskapet ikke har meldeplikt eller må ha personvernombud. Dette må forutsette at kollektivselskapet gir en motytelse til samtykket som er rettslig bindende, sannsynligvis av en viss monetær verdi, uten å bruke denne informasjonen til noe annet enn å oppfylle denne forpliktelsen.

Hvordan man kan innhente samtykke på gyldig vis defineres som tidligere nevnt<sup>168</sup> i stor grad av at samtykket skal være "en frivillig, uttrykkelig og informert erklæring"<sup>169</sup>. Som jeg har vært inne på i forrige kapittel er det nødvendig å vurdere gjennomførbarheten av dette kravet i forkant, men selve innhenting av samtykket er først aktuelt når behandlingsgrunnlag er valgt. For en behandlingsansvarlig som drifter et elektronisk billettsystem vil noe av utfordringen ligge i at kundedekontakten er relativt sporadisk. Dette kan gjøre det utfordrende å lage en registreringsrutine som sikrer gyldig samtykke. De fleste reiser og billett kjøp foregår uten omfattende kontakt med kundesenter eller kollektivselskapets representanter. Om man skulle gi oppgaven med å informere og samle inn samtykkeerklæringer til for eksempel bussjåfører, ville dette medføre forsinkelser og betraktelige ulemper for både reisende og ansatte. Dagens billettsalg foregår stadig oftere gjennom automater plassert på holdeplassen eller gjennom kioskkjeder. Å sikre at alle kioskansatte

---

<sup>168</sup> Se kapittel 3.5 med underkapitler.

<sup>169</sup> Jfr. popplyl § 2 nr. 7.

kjenner vilkårene og informerer kunder ved hvert eneste billett kjøp, ville vært en formidabel oppgave og lite realistisk å gjennomføre. Trolig vil det kun være mulig å kvalitetssikre at god og riktig informasjon blir gitt gjennom egne utsalgssteder knyttet til kollektivselskapet. Eksempler på slike utsalgssteder vil være Trafikanten, bussterminaler eller turistkontor.

Så lenge selskapet selger billetter andre steder, vil det neppe være tilstrekkelig å basere seg på salg av billetter som arena for tilstrekkelig informasjon og innhenting av samtykke. Trolig vil det være nødvendig at billetten i utgangspunktet anonym, og at kunden etter eget initiativ må knytte navn til billetten. Dette vil ikke være til hinder for at et samtykke kan registreres i direkte kontakt over disk. Det vil imidlertid forutsette et initiativ fra kunden for å forhindre at samtykke inngås passivt. Samtykke gjennom såkalt "negativ aksept"<sup>170</sup> vil sannsynligvis være ugyldig. Kunden vil trolig være mer mottakelig for informasjon i en situasjon der hun selv har tatt initiativet til registreringen. Trolig vil en eller annen form for elektronisk registreringsrutine være alternativet som gjør det lettest å sikre et gyldig samtykke.

Informasjonsplikten er en sentral del av å sikre at registreringsrutinen gir gyldig samtykke. Informasjonen skal gis den registrerte på eget tiltak dersom den samles inn fra den registrerte selv.<sup>171</sup> Jeg har tidligere slått fast at opplysninger som genereres gjennom bruk av elektronisk billett er å regne som samlet inn på denne måten.<sup>172</sup> Det er viktig å understreke at denne informasjonen må gis til den registrerte før det samtykkes til behandling av personopplysninger. Informasjonen må også være tydelig og bør helst skilles fra annen informasjon. Dette er ikke til hinder for at den behandlingsansvarlige kan gjøre den mest relevante informasjonen tydeligst og henvise til ytterligere informasjon for de som ønsker å sette seg inn i dette. Popplyls § 19 bokstav a-d bør allikevel anses som et minimumskrav til "umiddelbar informasjon". Denne informasjonen er av en karakter som bør være enkel å formidle kortfattet og oversiktlig. Popplyl § 19 bokstav d må trolig tolkes dit hen at det må informeres om at anonyme alternativer eksisterer.

Ved bruk av registrerte elektroniske billettsystemer, vil man vanligvis gi samtykke til å samle en ukjent mengde opplysninger på ubestemt tid, enten til bruken av kortet opphører eller samtykket trekkes tilbake. Konsekvensen for personvernet må sies å være uoversiktlige og omfanget av innsamlingen relativt stor. Det er derfor rimelig å anta at et samtykke til bruk av registrerte billetter bør inneholde en viss grad av skriftlighet. Det er ikke sikkert at selve samtykkeerklæringen må være skriftlig,<sup>173</sup> men det er rimelig å anta at informasjonen som gis i forkant er det. For eksempel i form av en brosjyre. Dette vil gi helt andre forutsetninger for å sette seg inn i, og forstå, konsekvensene av samtykket. Som jeg også har nevnt vil det i stor grad forenkle den behandlingsansvarliges arbeid med å sikre at tilstrekkelig informasjon alltid gis den

---

<sup>170</sup> Altså at fravær av svar eller mangel på protest mot registrering anses som aksept.

<sup>171</sup> Jfr. popplyl § 19 1. ledd.

<sup>172</sup> Ref. drøftelse i kapittel 3.5.2.

<sup>173</sup> For eksempel i form av en underskrift fra den registrerte.



registrerte.

I de tilfeller der registreringen foregår gjennom en nettside bør informasjonen gis i forkant av at den registrerte gir opplysninger til brukergrensesnittet. Dette innebærer at informasjonen må være tilgjengelig før det fylles ut noen form for skjema. Også dersom grensesnittet ber om en siste bekreftelse på at samtykke er gitt som et siste ledd i prosessen.

Popplyls § 19 bokstav e er ikke uttømmende og dermed åpen for tolkning. I en situasjon der samtykke gir grunnlag for behandling av personopplysninger på ubestemt tid, vil trolig informasjon om muligheten for tilbaketrekking<sup>174</sup> av samtykke være en forutsetning for å gjøre "den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte". Trolig bør det også informeres om fremgangsmåten for å gjøre både dette og be om innsyn eller sletting av opplysninger, samt konsekvensene av å trekke tilbake et samtykke. Dette blir særlig aktuelt i de tilfeller der henvendelsen må sendes et annet sted enn det som opplyses etter popplyl § 19 bokstav a.

Formuleringen i bokstav e omtaler spesifikt rettigheter etter loven. Sannsynligvis skal det mye til før behandlingsansvarlig plikter å informere på en måte som fremstår som advarsler. For eksempel å informere om mulige personvernkonsekvenser som kan oppstå som følge av samtykket.

Det er imidlertid grunn til å se på hvorvidt samtykkets krav til "informert" vil innebære et ansvar hos den behandlingsansvarlige for å sikre at den registrerte forstår potensielle konsekvenser av et eventuelt samtykke. Slik jeg ser det er det to kriterier som må vurderes i denne sammenhengen. Det første er hvor store konsekvenser for den registrertes personvern som følger av behandlingen og sannsynligvis også en vurdering av misbrukspotensiale innenfor rimelighetens grenser. Jo større konsekvens, jo mer informasjon bør den registrerte ha. Den andre vurderingen er hvorvidt disse konsekvensene er åpenbare og "logiske" i forhold til informasjonen som samles inn. Dersom formålet først og fremst skal gi anonym statistikk om reisefrekvens, billettyper og lignende og samtidig brukes til å tilby tilleggstjenester, vil det neppe være en selvfølgelighet at opplysningene kan brukes til å kartlegge den enkeltes bevegelsesmønster. På den annen side vil det kun kartlegges påstigningsholdeplassen og ikke destinasjonen. For periodebilletter er det heller ikke nødvendig å gi fra seg opplysninger hver eneste gang. Sammenlignet med informasjonen man kan hente fra for eksempel en mobiltelefon, vil det fremstå som ufullstendig og et lite egnet verktøy for en slik kartlegging.<sup>175</sup> De ufullstendige opplysningene gjør kartleggingen, og dermed personvernkonsekvensene, sterkt redusert. Dersom kollektivselskapet unngår å lagre opplysningene på en sånn måte at de er lette å sammenstille med den registrertes identitet, vil det neppe være stor risiko for at opplysningene blir brukt på en slik måte. Dermed er krav om å informere

---

<sup>174</sup> At samtykket kan trekkes tilbake kommer frem av Ot. Prp. Nr 92 (1998-99), s. 104.

<sup>175</sup> Kervarec, Varog og Kurt Lekanger (2012), "Så mye er lagret om deg".

om potensielle konsekvenser neppe aktuelt i forbindelse med elektroniske billettsystemer.

Som en følge av "informert"-kravet bør det også informeres om hvor lenge opplysningene lagres, hvorvidt de blir anonymisert i visse tilfeller<sup>176</sup> og hvorvidt det er mulig å få opplysningene slettet om man angrep.

Når den registrerte er tilstrekkelig informert, blir det viktig at det er tilrettelagt for innsyn for den registrerte.<sup>177</sup> Tekniske løsninger vil ofte kreve at slike vurderinger er gjort i forkant av at behandlingen av personopplysninger settes i gang slik at denne muligheten er integrert i systemet. Dersom innsyn skjer gjennom en henvendelse til en kundebehandler, bør systemet gjøre det mulig å hente opp relevant informasjon og så lite overflødig informasjon som mulig. Å legge til rette for innsyn vil også innebære at man er i stand til å svare på henvendelser innen 30 dager.<sup>178</sup>

Et annet teknisk krav er sletteplikten. Når opplysningene ikke lenger er nødvendige å beholde, skal de slettes i henhold til popplyl §§ 11 bokstav e og 28. Dette er et teknisk krav fordi informasjonsmengden er såpass stor at det sannsynligvis er nødvendig med en automatisk sletterutine for å sikre at kravet tilfredsstilles. Innunder sletteplikten følger også muligheten til å trekke tilbake et samtykke. Dersom samtykket blir trukket tilbake vil det innebære at opplysningene som er samlet inn må slettes. Å trekke tilbake samtykket bør rent teknisk være forholdsvis enkelt for den registrerte. Enten ved at den registrerte kan gjøre det selv, eller ved en enkel henvendelse.

Videre bør kollektivselskapet gi den registrerte tilgang til å rette mangelfulle opplysninger. Enkelte opplysninger kan det være formålstjenelig å la den registrerte redigere direkte. Den registrerte vil selv være den beste kilden til informasjon av typen navn, oppdatert adresse og telefonnummer. Andre typer opplysninger, som for eksempel reisedata, vil det være nødvendig å begrense tilgangen til. Om opplysningene skal brukes til statistiske formål kan statistikken ødelegges dersom den registrerte endrer eller sletter opplysninger. Kollektivselskapet har også en berettiget interesse i å kunne kontrollere opplysningene som regulerer varighet på billett og penger den registrerte har til gode. Det er ikke dermed sagt at den registrerte skal fratas enhver mulighet til å rette på informasjon som oppstår ved en eventuell datafeil eller lignende, men da gjerne indirekte, for eksempel gjennom en kundebehandler. En mulig bieffekt av at disse opplysningene er noe vanskeligere tilgjengelig er at det øker informasjonssikkerheten.

Den behandlingsansvarlige skal ha tilstrekkelig informasjonssikkerhet. I tillegg til å hindre uautorisert tilgang, innebærer det et krav til at innsamlede personopplysninger

---

<sup>176</sup> For eksempel når den brukes i statistikk.

<sup>177</sup> Retten til innsyn er regulert i popplyl § 18.

<sup>178</sup> Jfr. popplyl § 16.

ikke benyttes til annet enn det på forhånd uttrykte formålet.<sup>179</sup> Popplyl stiller en rekke krav til sikkerheten, blant annet i § 13. I tillegg skal det opprettes dokumenterbare rutiner for internkontroll etter popplyl § 14.

Dette er ikke en uttømmende liste over sikkerhets- og systemkrav. Jeg velger å nevne dem uten å gå i dybden da disse kravene ikke vil være gjenstand for undersøkelse i kapitlene 4 og 5. Fokus vil hovedsakelig ligge på de krav som oppleves av den registrerte og de krav som gjør henne i stand til å styrke eget personvern og praktisere egne rettigheter.

### 3.6.2 Oppsummering

Som vi ser av denne gjennomgangen er det en viss overlapp mellom enkelte av kravene. For eksempel vil en registreringsrutine som sikrer gyldig samtykke forutsette at informasjonsplikten er oppfylt. I enkelte tilfeller er jeg nødt til å ta utgangspunkt i informasjonen på nettsiden uten mulighet for å etterprøve påstandene. For eksempel vil jeg legge til grunn at det er lagt til rette for innsyn dersom det er lett å finne informasjon om hvordan dette gjøres og det tilsynelatende kan gjennomføres enkelt. "Samtykket er i utgangspunktet ikke tidsbegrenset."<sup>180</sup> i følge Ottesen og Blixrud, men det er uklart om dette også gjelder en situasjon der det jevnlig produseres nye opplysninger. Jeg har derfor valgt å ta med punktet "informeres det om samtykkets varighet?", men vil være forsiktig med å gi det avgjørende vekt i helhetsvurderingen av casene.

Basert på vurderingene i dette kapittelet har jeg kommet frem til følgende punkter jeg vil vurdere casene etter:

- Er informasjonen tydelig og lett å finne?
- Er informasjonen entydig?
- Er språket lett forståelig?
- Er formål formulert på forhånd?
- Er formål kommunisert til den registrerte?
- Er formål saklig begrunnet i bedriftens virksomhet?
- Er det informasjon om hvorvidt opplysningene blir utlevert til andre?
- Er det informasjon om hvorvidt det er frivillig å gi fra seg opplysningene?
- Informeres det om samtykkets varighet?
- Informeres det om lagringstid før opplysningene slettes?
- Er det informasjon om hvorvidt opplysninger anonymiseres?
- Er det anonyme alternativer tilsvarende registrert billett tilgjengelig?
- Er relevant informasjon gitt før den registrerte gir fra seg opplysninger?
- Krever samtykket en aktiv handling, eller er den innebygget i en annen prosess?

---

<sup>179</sup> Jfr. popplyl § 11 bokstav a-c.

<sup>180</sup> Ottesen og Blixrud (2010), s. 72.

- Er kontaktinfo til behandlingsansvarlig lett tilgjengelig?
- Er det lagt til rette for innsyn?
- Er det muligheter for å rette informasjon?
- Er det lagt til rette for å kunne trekke tilbake samtykke?
- Er det mulig å få opplysningene slettet?

### 3.7 Uforholdsmessig vanskelig å innhente samtykke?

Kravene til et gyldig samtykke kan oppleves som rimelig strenge, eller krever i det minste en omfattende vurderingsprosess fra den behandlingsansvarliges side. Samtykke er riktignok det foretrukne behandlingsgrunnlaget, men muligheten for å avvike fra samtykke oppstår når innhenting av samtykke blir for vanskelig. Som tidligere nevnt holder det ikke bare at det er kostbart eller lignende. Dersom kravene til samtykke i seg selv er for strenge, vil de kunne forårsake at terskelen for å benytte seg av andre behandlingsgrunnlag senkes. Om det skulle skje har kravene på sett og hvis fungert mot sin hensikt. Derfor er det viktig å balansere disse kravene med en forholdsmessighetsvurdering. Et sentralt moment blir å vurdere den enkeltes reelle behov for vern av opplysninger om en selv slik at kravene er, og oppleves som, rimelige. Både for den registrerte og den behandlingsansvarlige.

Å ta i bruk elektronisk billett forutsetter en eller annen form for kontakt mellom innehaver av kortet og kollektivtransportprodusenten. Hos mine to caser er det i essens to måter å skaffe seg et slikt kort på. Den ene er å kjøpe kortet over disk på spesielle utsalgssteder. I Innlandskortets tilfelle er dette primært på to utvalgte turistkontorer, samt to andre "skysskontorer" i følge Bjørn Rune Holmen<sup>181</sup>. I Reisekortets tilfelle er dette hovedsakelig Trafikanten og Oslo Sentralstasjon. Den andre måten, som er felles for dem begge, er å bestille kortet på nettsidene deres.

Med såpass få utsalgssteder skal det etter mitt skjønn være mulig å ha relativt god kontroll på hva slags informasjon som gis kunden ved kjøp, og registrering, av elektronisk billett. På nettsiden kan den nødvendige informasjonen enkelt gis ved for eksempel dialogbokser underveis i selve registreringsprosessen. Jeg vil tro at begge disse løsningene er mulig å legge opp på en slik måte at de tilfredsstiller vilkårene for reelt samtykke.

Det er med andre ord ikke belegg for å hevde at innsamling av samtykke vil medføre såpass stor ulempe eller kostnad at man lovlig kan sette samtykket til side og benytte seg av alternative behandlingsgrunnlag.

## 4.0 Dagens praksis hos Reisekortet

I de to følgende kapitlene vil jeg forsøke å svare på spørsmål 3 og 4 i problemstillingen min. Kapittel 4 og 5 vil ta for seg hvordan samtykke innhentes og hva slags informasjon som gis den registrerte hos henholdsvis Reisekortet og

---

<sup>181</sup> Teamleder IKT hos Oppland Trafikk.

Innlandskortet. Avslutningsvis i begge kapitlene vil jeg forsøke å vurdere praksisen opp mot kravene jeg kom frem til i kapittel 3.6.4.

Begge casene bruker egne nettsider som det viktigste kontaktpunktet for registrering av kort og øvrig informasjon om personopplysningsrelaterte tema. Jeg vil derfor først og fremst fokusere på nettsidene deres i denne vurderingen. Jeg kommer likevel til å supplere helhetsvurderingen med eventuell annen informasjon<sup>182</sup> jeg kan finne.

Det vil bli vanskelig for meg å svare uttømmende på hva slags praksis casene har for innsamling<sup>183</sup> av personopplysninger utover informasjonen som gis via nettsidene og hva jeg har blitt fortalt gjennom intervjuene. Inntrykket er at mesteparten av informasjonen som samles fra kundene genereres enten ved bruk av billettene, eller gjennom registreringsskjema på nettsidene. Ettersom jeg har begrenset mulighet til å teste praksis rundt alle krav loven stiller, vil jeg ta utgangspunkt i at informasjonen som gis stemmer. Om kollektivselskapet hevder de svarer på innsynsforespørsler innen en gitt tid, vil jeg forholde meg til dette som om det stemmer. I et slikt eksempel vil det allikevel være interessant å se på hvor enkelt det er å henvende seg og hvor lett tilgjengelig for eksempel kontaktinformasjonen er. Jeg er først og fremst på utkikk etter informasjon om personvern<sup>184</sup>, samtykke eller annen informasjon som kan bidra til å styrke den registrertes<sup>185</sup> kunnskap om egne rettigheter. Jeg vil først se helhetlig på hva som er tilgjengelig av relevant informasjon før jeg ser nærmere på selve registreringsrutinen<sup>186</sup>. Spesielt interessant er om informasjonen som gis tilfredsstiller kravene til et gyldig samtykke. Etter en gjennomgang av eventuelt annet tilgjengelig materiale, vil jeg drøfte praksis opp mot punktlisten i kapittel 3.6.2.

#### 4.1 Generelt om informasjon som gis på nettsiden

Reisekortets hjemmesider befinner seg på adressen [www.ruter.no](http://www.ruter.no). Jeg vil i løpet av dette kapittelet vise en del skjermdump<sup>187</sup>. De er først og fremst ment for å gi et inntrykk av hvor på nettsiden informasjonen befinner seg, altså hvor øyenfallende den er. Selve det tekstlige innholdet vil jeg forsøke å oppsummere i tekst.

Under er et skjermdump av forsiden på nettsidene. Det er to knapper/funksjoner som fører til informasjon om dine personvernrettigheter. Disse er markert med rødt.

---

<sup>182</sup> For eksempel brosjyrer eller beskrivelser av egen praksis i intervjuene jeg har gjort.

<sup>183</sup> Ref. første halvdel av spørsmål 3 i problemstillingen.

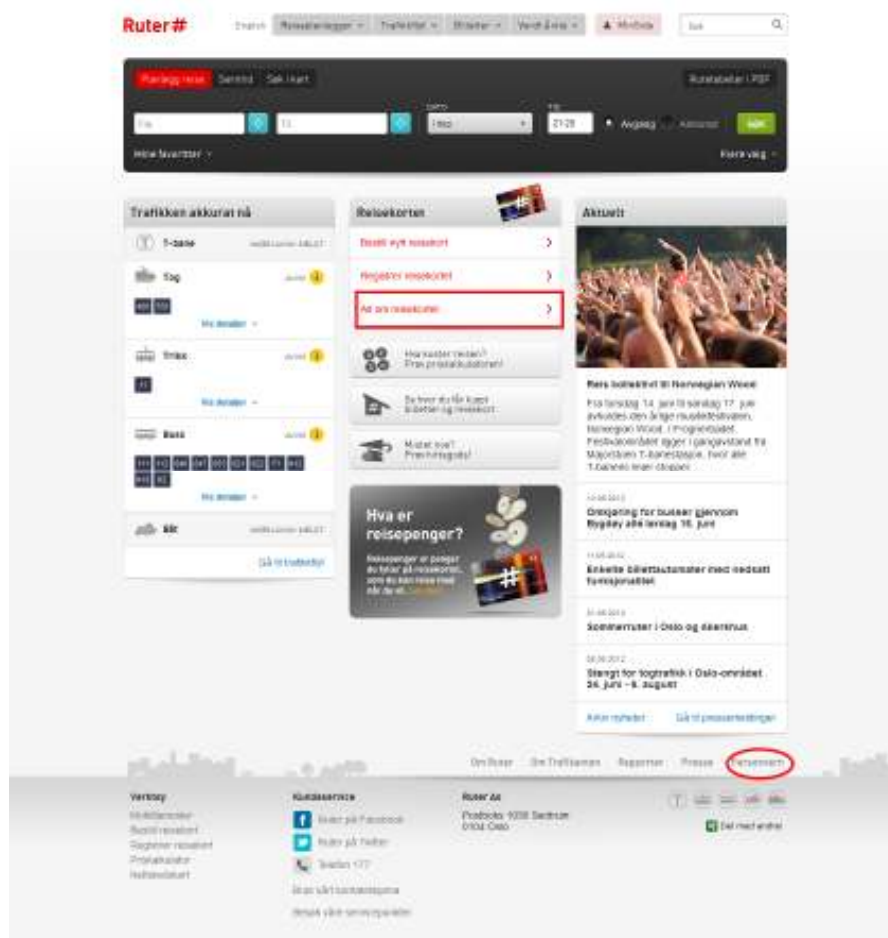
<sup>184</sup> I dette kapittelet vil begrepet "personvern" også bli brukt om informasjon som omhandler personopplysningsvern og henvisninger til personopplysningsloven.

<sup>185</sup> "Den registrerte" er i denne sammen også en person som ikke enda er registrert, men kan finne på å bli det. Dette fordi et gyldig samtykke krever at man er informert før registreringen finner sted.

<sup>186</sup> Altså prosessen for å knytte en identitet til sitt eget kort.

<sup>187</sup> Bilder av nettsidene tatt fra skjermen.

Bilde 1



Nederst på siden er det en rekke knapper om generelle tema. Knappen markert med rød sirkel er titulert "personvern". Denne lenker til en side med generell personverninformasjon. Personvern-knappen er gjennomgående på alle undersidene av ruter.no og alltid tilgjengelig på samme sted.<sup>188</sup>

Markert med en rød firkant er knappen "Alt om Reisekortet". Denne lenker til en informasjonsside om reisekortets mange muligheter. På nettsiden om Reisekortet finnes en rekke praktisk informasjon om bruken av Reisekortet.

<sup>188</sup> Den 01.07.2012 ble denne knappen fjernet fra nettsiden.

Bilde 2



Siden er organisert med en meny om populære temaer i margin til venstre. Denne menyen, som er markert med grønn firkant, går igjen på de fleste av undersidene, men er ikke på forsiden. Menyene inneholder ingen tema om registrering av kort eller personvern. Brødteksten på nettsiden om Reisekortet<sup>189</sup> er delt inn i 8 undertema. Mellom tema nummer 5 og 6 er det en rekke lenker til videoer. Tema nr. 6 forklarer at alle Ruters reisekort selges anonyme, og at dersom man ønsker kan man velge å

<sup>189</sup> Se bilde 2.

registrere dem. Den røde firkanten markerer en lenke til en nettside om registrerte kort. De to røde sirklene markerer lenker til nettsiden om personvern.<sup>190</sup>

Lenken i rød firkant fører til en nettside som innledningsvis informerer om fordelene ved å registrere kortet sitt.<sup>191</sup> Allerede nederst i andre avsnitt lenkes det på denne siden til informasjon om "personvern og registrering av kort". Siden inneholder lite om personopplysninger, men er den første nettsiden som eksplisitt opplyser brukeren om at det er valgfritt å registrere kortet. Også dette avsnittet inneholder en lenke til siden om personvern. Utover dette inneholder nettsiden stort sett opplysninger om fordelene ved registrering.

Nettsiden om personvern<sup>192</sup> består for det meste av tekst som er delt inn i tre hoveddeler:

- Elektronisk Reisekort
- Nettstedet ruter.no
- Trafikanten og Ruter på mobil

Informasjonen om Reisekortet er altså det første som er synlig for leseren. Teksten åpner med å fortelle at det er valgfritt å avgi personopplysninger og forklarer kort hvilke tjenester som tilbyr anonym reise. Videre står det litt om fordelene ved å registrere kortet sitt.

Neste avsnitt forsikrer om at Ruter ikke misbruker, samt sikrer opplysningene tilstrekkelig. Her er det også en lenke til personopplysningsloven hos Lovdata. Videre følger et avsnitt som i klartekst informerer om noen av den registrertes rettigheter, nærmere bestemt retten til innsyn, retting og sletting. Det er også kontaktinfo til kundeservice som kan benyttes til slike henvendelser. Det lenkes også til en egen nettside om "Ruters behandling av personopplysninger".<sup>193</sup>

Nettsiden om behandling av personopplysninger åpner med mye av den samme informasjonen leseren tidligere har blitt presentert for<sup>194</sup>, men har i tillegg ytterligere informasjon om selve behandlingen av personopplysninger. Også her er det lenket til personopplysningsloven og tidligere nevnte nettside om registrerte og uregistrerte kort. Dette er den første siden som sier noe om formålet med behandlingen av personopplysninger. Dette har riktignok vært implisitt tidligere, men uten bruken av ordet "formål". Tidligere tekst som omhandler behandling av personopplysninger har heller ikke fremstått som uttømmende og utelukket at opplysningene skal kunne brukes til andre ting. Her opplyses det om at "*hovedformålet [er] å kunne gi deg en best mulig oppfølging av ditt kundeforhold.*". Heller ikke dette er uttømmende, men det er den hittil mest nøyaktige informasjonen om hva opplysningene skal brukes til.

---

<sup>190</sup> Også denne ble fjernet 01.07.2012.

<sup>191</sup> Ruters hjemmesider, *MinSide* (2012).

<sup>192</sup> Ruters hjemmesider, *Personvern* (2012).

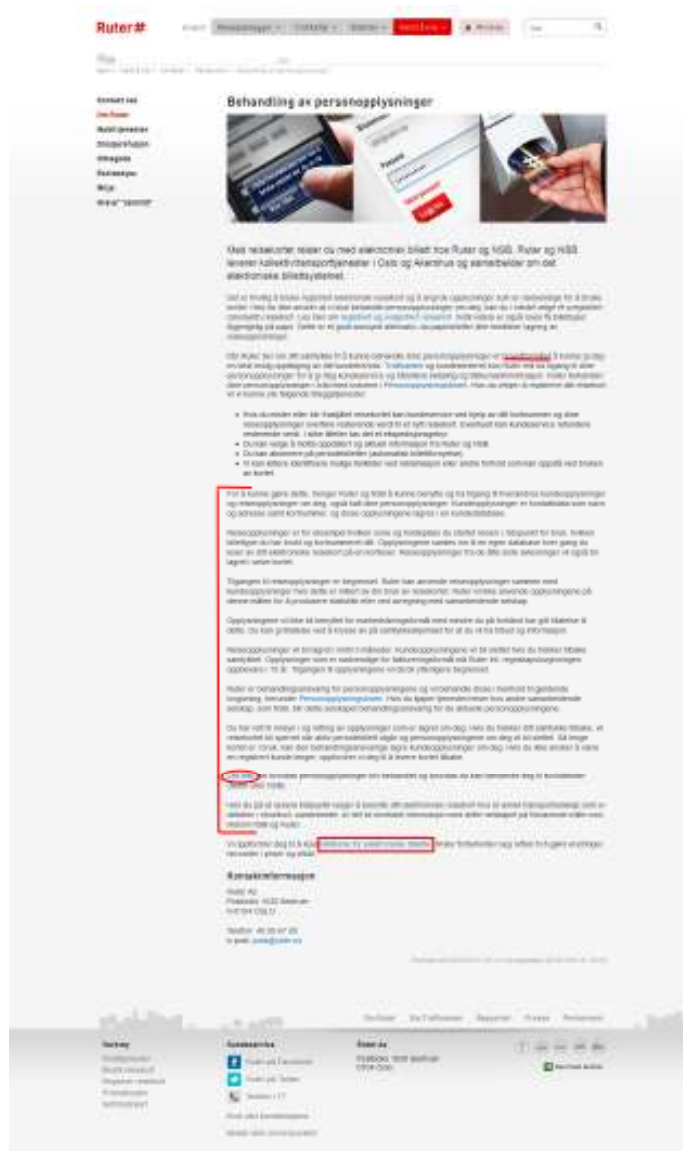
<sup>193</sup> Ruters hjemmesider, *Behandling av personopplysninger* (2012).

<sup>194</sup> Hele avsnitt er identiske ord for ord.



Etter en del informasjon om fordelene med registrerte kort, blir behandlingen utdypet ytterligere. Her nevnes det blant annet at Ruter og NSB har behov for å utveksle personopplysninger seg imellom, hvilke opplysninger som lagres og hvordan de lagres, at opplysningene ikke vil bli brukt til statistikk og hvor lenge de lagres. Jeg ramser ikke opp all informasjonen her, men har i skjermdumpet under markert med rødt hvilken del av teksten som inneholder ny informasjon om behandlingen av personopplysninger.

Bilde 3



Understrekingen markerer setningen der formålet er nevnt. Sirkelen er nok en lenke til den generelle siden om personvern og firkanten markerer en lenke til siden "om Reisekortet". Sistnevnte er denne gangen omtalt som "vilkårene for elektroniske billetter". "Klammen" plassert i venstre marg markerer en relativt omfattende sammenhengende tekst om behandling av personopplysninger, rettigheter og

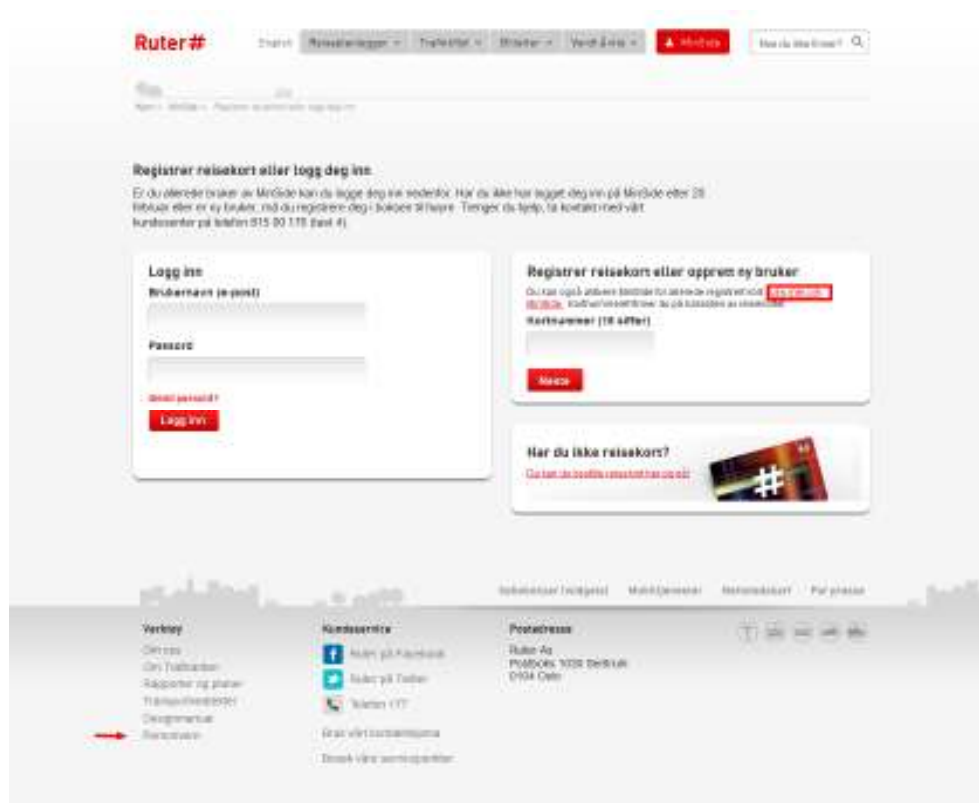
muligheter for den registrerte. Som jeg allerede har antydnet er dette den grundigste og mest informative teksten om personvern på ruter.no jeg har sett hittil.

## 4.2 Registreringsprosessen på nett

Skjermdumpene fra registreringsprosessen er tatt noen dager etter de andre skjermdumpene. I mellomtiden har Ruter endret hjemmesiden sin. Endringene ser ikke ut til å være store, men tidligere omtalte knapp om personvern i nettsidens "footer"<sup>195</sup> er fjernet. "Personvern" er ikke lenger en overordnet kategori på lik linje med for eksempel "nettstedskart", men er flyttet inn under kategorien "Om Ruter" som nederste underpunkt.<sup>196</sup>

Midtstilt på førstesiden på ruter.no, rett over knappen som er markert med rød firkant i Bilde 1, befinner knappen "Registrer Reisekortet" seg. Denne fører leseren til en nettside der man kan registrere uregistrerte Reisekort eller logge seg inn på Ruters tjeneste "MinSide" (sic) om man allerede har registrert Reisekort.

Bilde 4



Innlogging skjer ved bruk av e-postadresse og selvvalgt passord. For å registrere et nytt Reisekort må man taste inn kortnummeret på Reisekortet man ønsker å registrere og trykke "neste". Over feltet for kortnummer er det en tekst som informerer om muligheten for å logge seg på om kortet allerede er registrert. Det lenkes til et

<sup>195</sup> Footer er det faste bunnefeltet som er felles for alle nettsteder under et gitt domene.

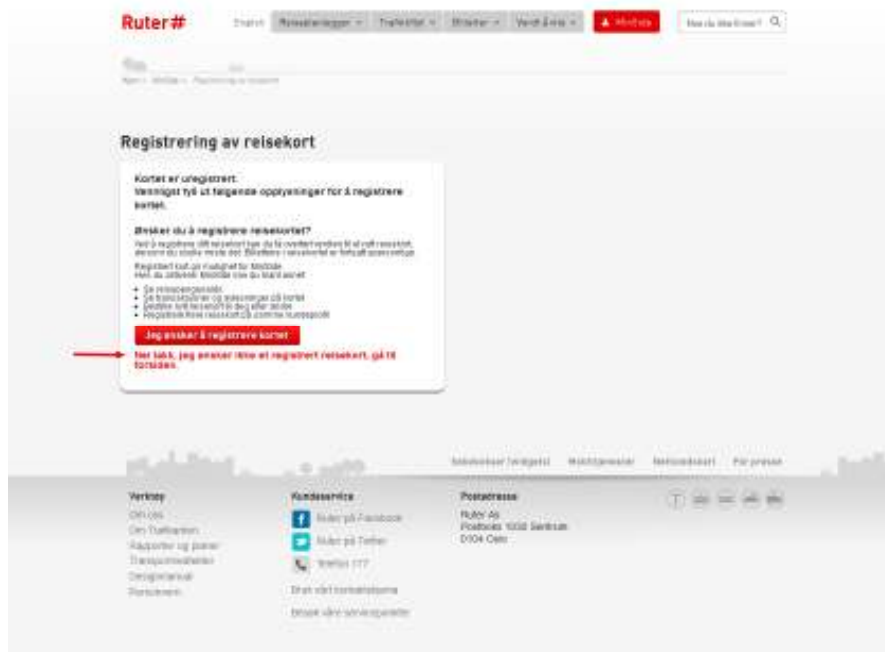
<sup>196</sup> Den nye plasseringen er markert med en rød pil i Bilde 4.

sted man kan lese med om "MinSide" (markert med rød firkant i Bilde 4) og informerer om hvor man finner kortnummeret.

Om man følger lenken markert med rød firkant får man kort informasjon om hvilke fordeler som følger med MinSide. Videre lenkes det til tidligere beskrevne nettside om personvern. Lenger ned på siden står det også at registrering er frivillig, men at tilleggstenester krever registrering.

Etter å ha tastet inn kortnummeret blir man henvist til en side som opplyser hvorvidt Reisekortet er registrert allerede eller ikke. Dersom kortet ikke er registrert får brukeren informasjon om fordelene ved å gjøre dette under overskriften "Ønsker du å registrere Reisekortet?".

Bilde 5



For å gå videre med registreringsprosessen kan man trykke på den røde knappen i Bilde 5. Rett under knappen står teksten "*Nei takk, jeg ønsker ikke et registrert reisekort, gå til forsiden.*". Denne teksten er en lenke til ruter.nos forside. Teksten er markert med en rød pil på bildet over.

Om man velger å gå videre via den røde knappen blir man presentert for et skjema som ber om en rekke opplysninger. I tillegg til Navn, adresse, poststed, postnummer, telefonnummer, e-post og fødselsdato må kunden bekrefte at hun er over 18 år gammel og at vedkommende samtykker til behandling av personopplysninger. Disse bekreftelsene skjer ved å "huke av" en boks ved hvert punkt.

Bilde 6

**Ruter#** | Search | Reisekort | Trafikk | Billetter | Verktøy | **MinSide** | Logg inn eller registrer

Registrering av reisekort

Kortet er uregistrert. Vennligst fyll ut følgende opplysninger for å registrere kortet.

**Navn \***

**Adresse 1 \***

**Adresse 2 \***

**Phone \*** **Postkode \***

☒ "Jeg besøker du i dag i over 18 år"

**Passordet (8-16 tegn A-Z a-z) \***

**Mobiltelnet \***

**E-postadresse \***

☒ "Jeg samtykker til at Ruter kan bruke mine personopplysninger som passord og e-post for å sende meg informasjon om tilbud og tjenester som er relevante for meg og min familie." **Jeg ønsker å motta tilbud fra NSB og Ruter**

☐ "Jeg samtykker til Ruter å bruke mine opplysninger for å sende meg informasjon om tilbud og tjenester som er relevante for meg og min familie." **Jeg ønsker å motta tilbud fra NSB og Ruter**

**Gjør du dette får du fullt registrert reisekort**

☒ "Jeg ønsker å motta tilbud fra NSB og Ruter"

**Ny e-postadresse \***

**Passord \***

**Gjenta passord \***

**Registrer kortet**

Søknader innleveret | Reiseressurser | Reiseressurser | For pressen

**Verktøy**  
 Kart  
 Kart  
 Kart  
 Kart  
 Kart  
 Kart

**Kundeservice**  
 Ruter på Facebook  
 Ruter på Twitter  
 Ruter på YouTube  
 Ruter på Instagram  
 Ruter på LinkedIn  
 Ruter på Nextdoor  
 Ruter på Messenger  
 Ruter på WhatsApp  
 Ruter på Telegram  
 Ruter på Signal  
 Ruter på WeChat  
 Ruter på Line  
 Ruter på KakaoTalk  
 Ruter på Viber  
 Ruter på Skype  
 Ruter på Zoom  
 Ruter på Jitsi  
 Ruter på Discord  
 Ruter på Slack  
 Ruter på Teams  
 Ruter på OneDrive  
 Ruter på SharePoint  
 Ruter på Yammer  
 Ruter på Lync  
 Ruter på Exchange  
 Ruter på Outlook  
 Ruter på Word  
 Ruter på PowerPoint  
 Ruter på OneNote  
 Ruter på Access  
 Ruter på Excel  
 Ruter på Publisher  
 Ruter på Word  
 Ruter på PowerPoint  
 Ruter på OneNote  
 Ruter på Access  
 Ruter på Excel  
 Ruter på Publisher

**Postadresse**  
 Ruter AS  
 Postboks 1000  
 0104 Oslo

Det er også mulig å samtykke til å motta tilbud fra NSB og Ruter, men dette er ikke påkrevet for å fullføre registreringen. Alle "bekreftelsesbokser" er blanke som standard når registreringen starter. Som et tilleggssvalg er det mulig å bekrefte at man ønsker tilgang til MinSide. Da må man i tillegg fylle inn e-postadresse en ekstra gang og ønsket passord. Det er uklart hvilke tjenester som er tilgjengelige om man velger å ikke få tilgang til MinSide.

Teksten ved boksen som bekrefter samtykke lyder som følger:

*"Ja, jeg samtykker til at Ruter kan behandle mine personopplysninger som beskrevet [her](#). Jeg er kjent med at det er frivillig å samtykke og at jeg når som helst kan trekke mitt samtykke tilbake."*

Den røde teksten er en klikkbar lenke og er markert med rød sirkel i Bilde 6. Lenken fører til en nettside som ikke eksisterer.<sup>197</sup>

Når registrering er fullført blir kunden tilsendt en e-post til valgt adresse og får beskjed om å bekrefte registreringen via denne. I e-posten blir kunden tildelt et kundenummer. Ruter informerer om at dersom registreringen ikke blir bekreftet innen 7 dager, blir informasjonen slettet. Ved å aktivere registreringen slik det beskrives i e-posten blir den registrerte henvist videre til en nettside som bekrefter at profilen er opprettet og kan deretter logge seg inn på MinSide ved hjelp av brukernavn og passord. Det er mye informasjon på MinSide om de forskjellige tilleggstenestene og muligheten for å sperre mistede kort. Det er ingen informasjon om behandling av personopplysninger, tilbaketrekking av samtykke eller personvern generelt.

Dersom man ønsker å trekke tilbake samtykket er det svært liten informasjon om dette på Ruters nettsider utover at det er mulig. Når man er pålogget på MinSide er det mulig å sperre kortet ved hjelp av en egen knapp, men ingen knapp som trekker tilbake samtykket eller sletter brukerens profil. Dersom man ønsker informasjon rettet eller slettet oppfordres det til å ta skriftlig kontakt.<sup>198</sup> Om man velger å redigere egen profil, får man muligheten til å rette på egen kontaktinformasjon. Boksen der man haker av for å samtykke til behandling av personopplysninger er også mulig å "redigere". Dersom man fjerner haken og lagrer, blir man spurt om man virkelig vil trekke tilbake samtykket og informert om at opplysninger fortsatt vil lagres til kortet utløper. I intervjuet med Ruters personvernombud, Svend Eric Wandaas, forklarer han at ved tilbaketrukket samtykke må kunden skaffe seg et nytt Reisekort, da det gamle vil bli ubrukelig.

Da jeg forsøkte å trekke tilbake samtykket på denne måten, fikk jeg ingen form for bekreftelse på at samtykket var trukket tilbake etter å ha svart bekreftende på om jeg ville trekke det tilbake. Jeg hadde fortsatt mulighet til å bruke tjenesten og slå opp informasjon om meg selv. Omtrent 5-6 dager senere ble tilgangen til MinSide borte og nettsiden responderte på mine innloggingsforsøk som om profilen aldri hadde eksistert. Da jeg noen uker senere forsøkte å registrere et annet Reisekort fikk jeg imidlertid beskjed om at e-postadressen jeg ville knytte til kortet allerede var i bruk.

---

<sup>197</sup> Ruters hjemmesider, *Behandling av personopplysninger* (2012).

<sup>198</sup> Denne informasjonen finnes på nettsidene om personvern, ikke på MinSide.

### 4.3 Andre kilder til informasjon

Jeg har fått se et begrenset utvalg av flygeblader, pamfletter og lignende utgitt av Ruter. Jeg har valgt å kalle utvalget begrenset fordi Wandaas fortalte om en infolapp som inneholdt informasjon om personopplysninger og samtykke. Denne har jeg ikke klart å finne. Ingen av de andre fysiske informasjonskildene jeg har sett inneholder noe om personopplysninger i forbindelse med Reisekortet. Det informeres kun om at henvendelser til Ruter kan bli lagret. For eksempel om man tar kontakt via telefon eller e-post.

I Ruters bok "Priser og billetter" er det på side 20 noe informasjon under overskriften "Hvordan du skaffer deg Reisekort". Her kommer det frem (implisitt) at det er frivillig å registrere kortet. Det oppfordres også til å lese av kortet hver eneste gang man bruker kollektivtransport, samt merke uregistrerte kort med navn eller andre kjennetegn.

Ved henvendelse hos for eksempel Trafikanten vil kundebehandleren kunne finne informasjon om dine reiser og din profil via datasystemet sitt i følge Wandaas. Trolig også tidligere henvendelser. Informasjonen hentes fra to separate databaser og sammenstilles kun på saksbehandlerens skjerm. Etter behandling lagres det ikke i sin sammenstilte form.

Det er grunn til å notere seg at majoriteten av registreringer skjer gjennom nettsiden, og at den derfor må anses som primær informasjonskilde. Svakheter ved informasjonen i det skriftlige, fysiske materialet vil neppe få konsekvenser for mange mennesker.

### 4.4 Drøftelse av Reisekortets praksis

Jeg vil nå først oppsummere mitt generelle inntrykk av nettsidene. Hovedfokus vil være på informasjonen som er viktig i forkant av at samtykke gis, både hvorvidt den er det, hvor lett tilgjengelig den er og hvor forståelig den fremstår. Deretter vil oppsummere selve registreringsprosessen. Til slutt vil jeg se på øvrig informasjon som er relevant for den registrerte i etterkant at samtykke er inngått.

At det alltid befinner seg en lenke til sidene om personvern i bunnfeltet<sup>199</sup>, er positivt og gir inntrykk av at temaet er ansett som viktig eller i det minste sentralt. Samtidig er dette et område på nettsidene som er langt mindre synlig enn menyene i toppfeltet eller den faste følgemenyen på venstre side.<sup>200</sup> At knappen "Personvern" er mørk grå på en lys grå bakgrunn, bidrar heller ikke til synlighet. Kun spesielt interesserte vil nok komme til denne siden via bunnfeltet.

Knapp til nettsiden "alt om reisekortet" er plassert godt synlig på ruter.nos forside.<sup>201</sup> Knappene "Bestill nytt Reisekort" og "Registrer Reisekortet" er de to forrige

---

<sup>199</sup> I forbindelse med programmering av nettsider er det dette som kalles en "footer".

<sup>200</sup> Følgemenyen er markert med grønt på Bilde 2.

<sup>201</sup> Markert som med rød firkant på Bilde 1.

alternativene på forsiden. Også dette er lagt opp på en slik måte at dersom man ikke på forhånd er oppmerksom på mulige problemstillinger eller utfordringer for personvernet, er det liten sjanse for at informasjonen på noe punkt fanger leserens øye.

Om man trykker for knappen om registrering av Reisekortet, kommer man til en nettside som starter registreringsprosessen og gir mulighet for innlogging på en "Min Side"-løsning<sup>202</sup> dersom kortet allerede er registrert. Denne siden gir ingen informasjon knyttet til samtykke eller personvern.

Alle sidene med relevant informasjon lenker til hverandre i en slags asymmetrisk sirkel. Dette sikrer at uavhengig av hvordan man finner dem vil all informasjonen være synlig eller henvist til. Enten det er "hovedveien" via forsiden, søkefeltet internt på siden, tilsendt direktelenke eller gjennom søkemotorer. Samtidig bidrar dette også til at noe av informasjonen fremstår som bortgjemt. Det krever mer av den registrerte å finne fram til den.

At personvern ikke er det fremste temaet på forsiden er naturlig, men også sider som handler om reisekort bærer preg av å gjemme bort informasjonen om personvern. De er preget av repetisjon og informasjon om fordelene ved registrering. På siden "alt om reisekortet" er det lenker videre til informasjon om personvern, men også dette er langt ned på siden. Over denne teksten er det en del praktisk informasjon som blant annet inneholder en anbefaling om å alltid validere kortet<sup>203</sup>. Et godt stykke nede på siden er det flere videoer som kan spilles av. Layouten gir inntrykk av at dette er nederst på siden. Om man blar seg ned forbi dette, finner man lenken til personvernsiden.<sup>204</sup>

Jeg vil trekke frem at siden om personvern umiddelbart knytter Reisekortet opp mot temaet som noe positivt. Det er også lenket til personopplysningsloven og ytterligere informasjon om behandling av personopplysninger fra denne siden.

Siden "om behandling av personopplysninger"<sup>205</sup> fremstår overordnet som meget grundig og utfyllende. Spesielt merket jeg meg følgende setning: *"Opplysningene vil ikke bli benyttet for markedsføringsformål med mindre du på forhånd har gitt tillatelse til dette. Du kan gi tillatelse ved å krysse av på samtykkeskjemaet for at du vil ha tilbud og informasjon."*

Denne setningen bidrar til å fjerne enhver tvil som måtte være der rundt selve samtykket til bruk i markedsføring. Dette er et selvstendig samtykke, tydelig adskilt fra det generelle samtykket til behandling av personopplysninger, og ikke "bakt inn" i en lengre avtaletekst. Teksten fremstår som ryddig og lett forståelig.

---

<sup>202</sup> Altså en innloggingstjeneste som er knyttet til den registrerte som person og de kortene hun har valgt å registrere. Det er ikke mulig å opprette en slik profil uten å knytte noen kort til den.

<sup>203</sup> Og dermed generere personopplysninger dersom kortet er registrert.

<sup>204</sup> Se Bilde 2.

<sup>205</sup> Se Bilde 3.

Selv om summen av informasjon på denne siden er god, er det fortsatt uklarheter også her. Eneste stedet formålet er nevnt eksplisitt er på denne siden. Det omtales som at *"hovedformålet [er] å kunne gi deg en best mulig oppfølging av ditt kundeforhold."*, noe som neppe kan anses for å være uttømmende. Videre står det at *"ruter må ha tilgang til dine personopplysninger for å kunne gi deg kundeservice og håndtere betaling og fakturaadministrasjon"*. Det forklares ikke at dette er i forbindelse med abonnementsløsninger eller betaling over internett. Det er også uklart hva det vil si å *"gi deg kundeservice"*, men det er neppe slik at man må ha personopplysninger for dette. Jeg har som nevnt ikke vært i stand til å finne at det er meldt formål inn til Datatilsynet og dermed er det vanskelig å vite om det er formulert et formål i forkant av behandlingen.<sup>206</sup> I utgangspunktet er behandlingsansvarlig pliktig til å melde inn formålet til Datatilsynet,<sup>207</sup> men tilsynet kan gjøre unntak fra meldeplikten dersom det istedenfor opprettes et personvernombud.<sup>208</sup> Jeg kjenner ikke til om Datatilsynet har gjort dette, men min kontaktperson hos Ruter<sup>209</sup> er på tilsynets liste over personvernombud<sup>210</sup>. Jeg velger derfor å legge til grunn at det er gitt unntak fra meldeplikten.

Hvorvidt formålet er saklig begrunnet i bedriftens virksomhet<sup>211</sup> er vanskelig å vurdere på grunn av utydeligheten i teksten som omhandler formålet. Det er definitivt slik at de fleste nevnte punktene henger logisk sammen med driften av kollektivselskap. Samtidig kan nevnte påstand om at kundeservice generelt krever personopplysninger neppe sies å være *saklig* begrunnet. Jeg er usikker på om saklighetskravet kun innebærer at formålet må være relatert til virksomheten eller om det også forutsetter en vurdering om hvorvidt det er nødvendig. Det er også mulig jeg legger for mye vekt på en utydelig kommunisert formål, og at det er grunn til å tolke denne formuleringen i "beste mening". Det er imidlertid lett å fastslå at formålet med hell kunne vært tydeligere kommunisert.

På nettsiden om behandling av personopplysninger informeres det om at opplysningene deles med NSB. Den samme siden er veldig tydelig på at det er frivillig å gi fra seg opplysninger og hvor lenge opplysningene blir lagret<sup>212</sup>. Det informeres ikke om samtykkets varighet noe sted, men nevnes dersom det trekkes tilbake blir opplysningene slettet. Dermed er det underforstått at samtykket er gitt på ubestemt tid.

Anonymisering av opplysninger er ikke omtalt, men det nevnes at kortene i utgangspunktet er anonyme ved førstegangskjøp.<sup>213</sup> Ruter forsikrer også om at

---

<sup>206</sup> Se kapittel 3.4.1. om formålet med behandlingen.

<sup>207</sup> Jfr. popplyl § 31.

<sup>208</sup> Jfr. personopplysningsforskriften § 7-12.

<sup>209</sup> Svend Eric Wandaas som jeg også intervjuet.

<sup>210</sup> Datatilsynet, *Alfabetisk oversikt over personvernombudene(2011)*.

<sup>211</sup> Jfr. popplyl § 11 bokstav b.

<sup>212</sup> 3 måneder som standard, bortsett fra opplysninger som er relevant for regnskap da disse lagres i 10 år.

<sup>213</sup> Dette står på nettsiden "om reisekortet".



reiseopplysninger ikke vil bli benyttet til å lage statistikk. Dermed er det neppe noe behov for anonymisering så lenge opplysningene ellers slettes som beskrevet. Jeg har heller ikke funnet eksempler på billetter som kun tilbys til registrerte kort. Fordelene med å registrere er først og fremst av praktisk og ikke økonomisk art.

Språket på nettsiden er godt og lettlest hele veien, men dessverre er noe informasjon vanskelig å finne og tidvis pakket inn i argumenter for å registrere seg. Generelt er altså nettsiden tydelig i tekst, men utydelig og tidvis villedende i sin struktur. Jeg tolker lovens krav til samtykke dit hen at den registrerte skal informeres om problemstillinger, rettigheter og potensielle personvernutfordringer. Også dersom hun ikke kjenner problemstillingene fra før av. Da blir det viktige å se på hvordan nettsidene informerer brukerne om sine rettigheter i en registreringsprosess. Altså hvorvidt konteksten rundt samtykke henleder den registrerte i retning av informasjonen på en god og opplysende måte.

Innledningsvis i kapittel 4.2 trakk jeg frem lenke til sidene om personvern i footeren som noe positivt. Også under registreringsprosessen er denne delen av nettsiden fast til stede. Dessverre ble lenken flyttet i løpet av de få dagene fra jeg sikret skjermdump av øvrige deler av nettsiden til jeg sikret skjermdump av registreringsprosessen. Lenken er nå langt mindre synlig og lenger ned på siden. Bunnfeltet som inneholder lenken var utenfor skjermbildet stort sett gjennom hele registreringsprosessen. Ved enkelte anledninger ville lenken vært synlig på sin gamle plass. Resultatet er at informasjonen i mindre grad er tilgjengelig. En såkalt footer, eller bunnfelt på en nettside er sjelden designet for å støtte en bestemt del av siden. Den skal være en generell snarvei og informasjon om de mest etterspurte temaer. Det er heller ikke rimelig å forvente at denne skal være den primære informasjonskilden til noe enkeltstående tema. Derfor blir det viktigere å vektlegge informasjonen som gis under selve registreringsprosessen. Ettersom det meste av relevant informasjon er samlet på tre nettsider som henviser til hverandre, blir dette først og fremst et spørsmål om å vurdere hvorvidt det er henvises til disse sidene på en god måte.

I Bilde 4 har jeg markert en lenke til en side som gir informasjon om MinSide. Lenken er en del av følgende tekst:

*”Du kan også aktivere MinSide for allerede registrert kort. [Les mer om MinSide.](#)  
Kortnummeret finner du på baksiden av reisekortet.”*

Denne teksten er den første i registreringsprosessen som kan lede kunden til informasjon om personvern eller behandling av personopplysninger. Selv om siden inneholder noe informasjon om selve registreringen samt noe informasjon om hvor man kan lese mer om personvern, er det lite i den henvisende teksten som tilsier dette. Teksten henvender seg primært til de som allerede har registrert et kort og sekundært til de som ønsker å vite mer om selve tjenesten MinSide. Det er tvilsomt om denne informasjonen i sin nåværende form kan sies å bidra til at samtykket er informert i særlig grad.

I Bilde 5 har jeg markert en tekst der man kan velge å ikke registrere kortet. Teksten er markert med en rød pil. Denne informasjonen er ikke knyttet direkte til samtykket, men den sier i det minste implisitt at registreringen er frivillig.

På selve registreringsskjemaet (Bilde 6) er den første virkelig relevante informasjonen. Det kanskje viktigste på denne siden er at det å gi samtykke er en aktiv handling og ikke en passiv del av en registreringsprosess for å oppnå noe annet. Dette gjøres ved å huke av boksen ved siden av samtykketeksten jeg siterte i kapittel 4.2. Det informeres klart og tydelig om at samtykke er frivillig og at samtykket kan trekkes tilbake. Det mest sentrale er likevel at man samtykker til behandling av personopplysninger i henhold til retningslinjer Ruter har beskrevet nærmere på en annen side dersom kunden ønsker å fordype seg i dette. Dessverre lenker denne teksten til en nettside som ikke eksisterer hos Ruter. Trolig skal lenken henvise til siden om personvern eller siden om behandling av personopplysninger. Begge disse sidene er omtalt grundigere i kapittel 4.1. Uten denne lenken inneholder ikke registreringsprosessen noe detaljert informasjon om hvilke opplysninger som behandles, hvorfor de behandles eller hvor lenge de behandles. Forhåpentligvis er dette en midlertidig feil som rettes opp. I så fall vil man nok kunne hevde at tilstrekkelig informasjon gjøres tilgjengelig i forkant.

I selve tjenesten MinSide er det ingen menyvalg som gir deg kontaktinfo til Ruter, men i footeren er det lenker til både facebookside og twitterkonto, telefonnummer og postadresse. Dette er også et relativt vanlig område å finne en "kontakt oss"-knapp på de fleste nettsider og må anses som et naturlig sted å lete etter slik informasjon.

MinSide gir god oversikt over hvilke elektroniske spor du har lagt igjen de siste 3 månedene,<sup>214</sup> samt hvilke transaksjoner det er gjort i forbindelse med kortet. Det er imidlertid ikke mulig å se hvilken holdeplass kortet ble brukt på. Denne tjenesten gir altså ikke innsyn i all informasjonen som er lagret om deg, kun den som anses som praktisk interessant. Det er ikke informert noe sted om muligheten til innsyn, men som nevnt er kontaktinfo relativt lett tilgjengelig. Det er også muligheter for å rette kontaktinformasjon og lignende. Som jeg har vært inne på tidligere har Ruter en berettiget interesse i å ikke gi kundene fri tilgang til å rette på trafikkdata.

I kapittel 4.2 beskriver jeg også prosessen med å trekke tilbake samtykke. Det er ingen forklaring på hvordan det gjøres og ingen bekreftelse på at det er gjennomført. Trolig vil en henvendelse til kundesenteret gi den veiledningen man trenger. I intervju med Wandaas forklarte han at tilbaketrekking av samtykke gjør kortet ubrukelig. Man må altså skaffe seg nytt anonymt kort, noe som begrunnes i tekniske begrensninger. I lys av at e-postadressen min "ble husket" av nettsiden, er dette urovekkende. Det kan tyde på at opplysningene ikke er mulige å anonymisere, og ettersom vi vet at noe ikke blir slettet, er det gode muligheter for at det ligger informasjon lagret som kan knyttes til e-postadresse til tross for at samtykke er trukket tilbake. Dette er det

---

<sup>214</sup> Ruter informerer på nettsidene at de sletter reiseopplysninger som er eldre enn 3 måneder.

vanskelig å få bekreftet, men dersom det er tilfelle, er det et relativt grovt overtramp mot den registrertes personvern. Det bør legges til at jeg oppdaget dette ved en tilfeldighet og at det i en normal situasjon ikke vil være grunn til å mistenke at ikke alt er som det skal. Den registrerte har med andre ord liten muligheten til å ta tak i dette på egne vegne.

Avslutningsvis bør det nevnes at NSBs nettsider ikke informerer om reisekortet eller personvern på forsiden. Det er mulig å søke seg frem til en nettside om vilkår for Reisekortet. Denne gir meget lite info. Dersom man benytter seg av adressen flexus.no,<sup>215</sup> blir man sendt til ruter.no. Ettersom Ruter er firmaet som stort sett presenterer billettsystemet i media, henvisninger på nett stort sett sendes til Ruter og NSB ikke informerer i særlig grad, har jeg valgt å ikke gå nærmere inn på NSBs informasjon i denne oppgaven.

---

<sup>215</sup> Flexus var navnet på de elektroniske billettene til Ruter og NSB før de skiftet navn til Reisekortet.

#### 4.5 Oppsummering av reisekortets praksis

Basert på drøftelsene i kapittel 3 har jeg laget en oversikt over sentrale krav jeg mener må oppfylles for at behandlingsgrunnlaget skal være lovlig. Kravene får en poengsum fr 0-2 der 0 er ikke oppfylt, 1 er delvis oppfylt og 2 er oppfylt. Under tabellen vil jeg kort redegjøre for hovedtrekkene og begrunne poengsummen på enkelte punkter.

Krav	Oppfylt
Er informasjonen tydelig og lett å finne?	1
Er informasjonen entydig?	1
Er språket lett forståelig?	2
Er formål formulert på forhånd?	1
Er formål kommunisert til den registrerte?	0
Er formål saklig begrunnet i bedriftens virksomhet?	1
Er det informasjon om hvorvidt opplysningene blir utlevert til andre?	2
Er det informasjon om hvorvidt det er frivillig å gi fra seg opplysningene?	2
Informeres det om samtykkets varighet?	1
Informeres det om lagringstid før opplysningene slettes?	2
Er det informasjon om hvorvidt opplysninger anonymiseres?	N/A
Er det anonyme alternativer tilsvarende registrert billett tilgjengelig?	2
Er relevant informasjon gitt før den registrerte gir fra seg opplysninger?	0
Krever samtykket en aktiv handling, eller er den innebygget i en annen prosess?	1
Er kontaktinfo til behandlingsansvarlig lett tilgjengelig?	2
Er det lagt til rette for innsyn?	1
Er det muligheter for å rette informasjon?	2
Er det lagt til rette for å kunne trekke tilbake samtykke?	0
Er det mulig å få opplysningene slettet?	1

Som vi ser av tabellen, er det ikke alle krav oppfylt, og blant de kravene som er oppfylt er det varierende grad av forbedringspotensiale. Stort sett er informasjonen

som gis skrevet på en oversiktlig og fin måte. På enkelte punktene er teksten krystallklar<sup>216</sup>. Min største innvending er at informasjonen er noe bortgjemt og ofte gjemmes bak argumentasjon for fordelene ved registrering. Ottesen og Blixrud hevder at "Frivilligheten vil også kunne trekkes i tvil dersom det knyttes for positive følger til det å samtykke"<sup>217</sup>. Samtidig blir det urimelig å tolke informasjonsplikten dit hen at selskapet ikke har lov å fremstille tjenesten sin fra sin beste side. Det er en svært vanskelig avveining mellom kundens behov for informasjon som gir realistiske forventninger og selskapets behov for å fremstå "tiltalende". Det blir trolig for mye å kreve at eventuelle personvernkonsekvenser skal fremstå som advarsler eller lignende. Dermed må mye av informasjonen som er gitt anses som tilstrekkelig ovenfor lovens krav, men i et personvernperspektiv er det definitivt rom for forbedring.

Personvern som tema er til stede på nettsiden og nevnes i såpass mange sammenhenger at det likevel skal være relativt enkelt å lete seg frem til dette. Ettersom Ruter har personvernombud, har jeg lagt til grunn at de ikke trenger å melde formålet inn for datatilsynet. Dermed har de fått "1" på dette punktet.<sup>218</sup> I mine øyne er imidlertid formålet ikke kommunisert på en slik måte at det er mulig for den registrerte å sette seg fullstendig inn i hva personopplysningene blir brukt til. Etter mitt skjønn er ikke dette godt nok kommunisert. Når det gjelder punktet om anonymisering, har jeg valgt å skrive N/A<sup>219</sup> ettersom Ruter informerer om at de ikke benytter opplysningene til utforming av statistikk. Ruter behandler ikke personopplysninger til noe formål som tilsier anonymisering.

Jeg har også valgt å konkludere med at det ikke gis tilstrekkelig med informasjon før man gir fra seg informasjon, som i dette tilfellet også innebærer å samtykke til behandling av personopplysninger. Det er mulig å se lenker til relevant informasjon i løpet av registreringsprosessen, men henvisningen er svært villedende og fremstår ikke som relevant for uregistrerte kort. Trolig ville lovens krav vært tilfredsstillt dersom den lenken i "samtykketeksten" hadde fungert. Forhåpentligvis er dette en midlertidig glipp som raskt rettes opp.

I mine øyne er det den mest alvorlige svikten i forhold til lovens krav knyttet til nest siste punkt på listen. Å finne ut hvordan samtykke kan trekkes tilbake er svært vanskelig og lite intuitivt. I tillegg er det manglende bekreftelse på at samtykke er trukket tilbake. Når det i ettertid viser seg at e-postadressen min fortsatt er lagret i systemet, til tross for tilbaketrukket samtykke, er dette neppe tilstrekkelig. Jeg har allikevel valgt å gi muligheten for å slette opplysningene karakteren 1. Dette fordi

---

<sup>216</sup> På disse punktene har jeg gitt "karakteren" 2.

<sup>217</sup> Ottesen og Blixrud (2010) s. 73.

<sup>218</sup> Formålene som formidles er såpass generelle at de kan gi inntrykk av å være formulert i etterkant for å dekke det meste av behandlingen som gjøres. Dette er det selvsagt umulig å slå fast, men det er bakgrunnen for at dette punktet ikke fikk karakteren "2".

<sup>219</sup> N/A står for "Not applicable" og er en vanlig betegnelse å bruke der informasjon ikke er relevant eller passer inn.

Ruter også oppfordrer til skriftlig kontakt for retting og sletting på nettsidene sine. Dermed legger jeg til grunn at en manuell behandling vil kunne løse dette problemet.

Selv om registreringsrutinen ikke får godkjent på alle punkter, er det relativt små endringer som skal til for å tilfredsstille kravene jeg har vurdert den etter. Trolig vil det vanskeligste være å løse tilbaketrekkingen av samtykke ettersom det sannsynligvis vil kreve endring i programmeringen og ikke bare redigering av tekst eller retting av døde lenker.

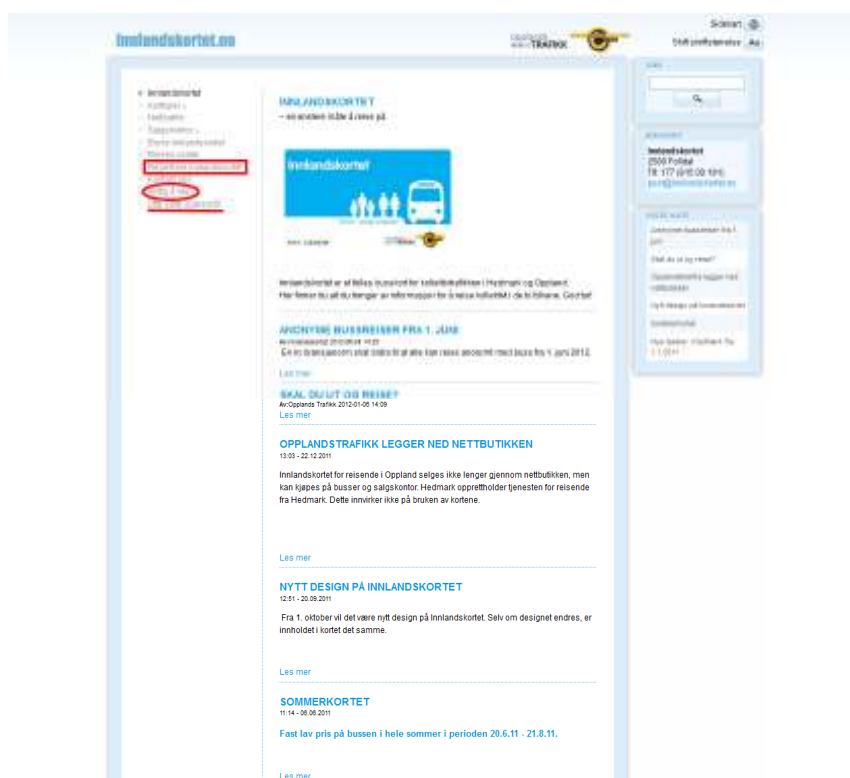
## 5.0 Dagens praksis hos innlandskortet

Innlandskortet er som kjent et samarbeid mellom Hedmark Trafikk og Oppland Trafikk. Begge selskapene har egne nettsider, men mitt fokus vil ligge på den felles nettsiden innlandskortet.no. HT og OTs nettsider henviser også til denne nettsiden om temaer som personvern og registrering av kort.

### 5.1 Generelt om informasjon som gis på nettsidene

Forsiden på innlandskortet.no inneholder ingen henvisning direkte til temaer om behandling av personopplysninger eller personvern. Nettsiden har ikke fast bunnfelt med knapper som følger leseren gjennom alle sidene.

Bilde A<sup>220</sup>

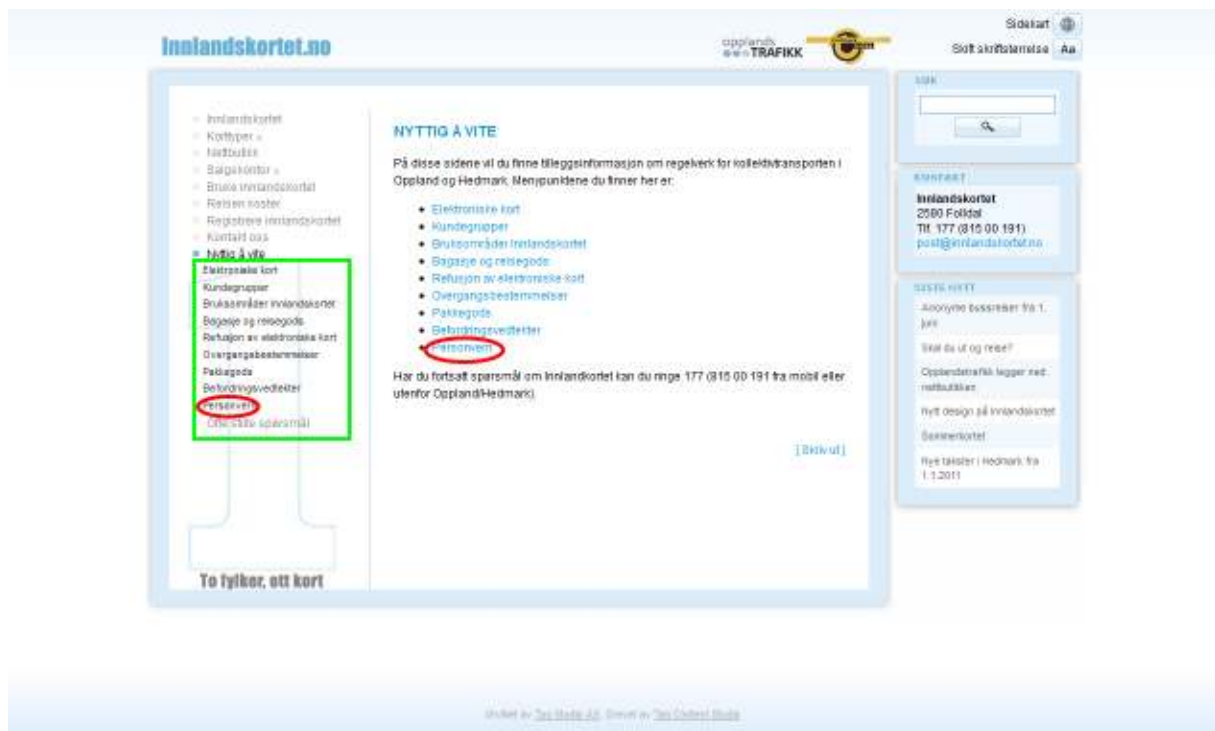


<sup>220</sup> Nettsiden hadde flere nyhetsoppslag enn det som er synlig på bildet, men ingen informasjon utover dette. Bildet er kuttet av plasshensyn.

I venstremargen på nettsiden er det en fast meny som følger leseren gjennom alle sidene. Enkelte av knappene i denne menyen har underkategorier som blir synlige om man klikker på det overordnede temaet. I menyen befinner det seg blant annet en knapp som lenker til en side for å "registrere innlandskortet"<sup>221</sup> (markert med rød firkant), "Nyttig å vite"<sup>222</sup> (markert med rød sirkel) og "Ofte stilte spørsmål"<sup>223</sup> (understreket med rødt). Førstnevnte tar leseren rett til registreringsprosessen. Selve startsidene for registreringsprosessen inneholder en rekke felter som kan fylles ut, men ingen informasjon om behandling av personopplysninger eller lignende.

Under "nyttig å vite" blir vi presentert for ni forskjellige temaer. Det siste temaet av de ni er "personvern"<sup>224</sup>. Menyene i venstremargen blir også utvidet med disse ni temaene så lenge man befinner seg på nettsiden for noen av disse (markert med grønn firkant i Bilde B).

Bilde B



Dette innebærer at selv om leseren skulle finne et av de tidligere temaene interessante, vil personvern (markert med rød sirkel) fortsatt være til stede til venstre på siden.

På nettsiden om personvern er det aller først en anbefaling om å registrere kortet sitt. Dette begrunnes med at kollektivselskapene skal kunne gi brukeren tilleggstjenester som rekonstruksjon av tapte kort eller refusjon ved tap av kort. Det informeres også

<sup>221</sup> Innlandskortets hjemmesider, *Registrering* (2012).

<sup>222</sup> Innlandskortets hjemmesider, *Nyttig å vite* (2012).

<sup>223</sup> Innlandskortets hjemmesider, *Ofte stilte spørsmål* (2010).

<sup>224</sup> Innlandskortets hjemmesider, *Personvern* (2012).

om hvilke typer opplysninger som lagres ved bruk av kortet. Det virker ikke som oversikten er utførmende. Videre opplyses det om at behandlingen krever samtykke og at det er valgfritt å registrere seg.

Til slutt på nettsiden ramses det opp noen flere fordeler ved å registrere seg før følgende punktliste presenteres:

*"Hensynet til ditt personvern er svært viktig for oss i Opplandstrafikk. Derfor lover vi at:*

- *Du skal ha god informasjon om hva vi bruker dine personopplysninger og reisedata til*
- *Alle personopplysninger skal lagres sikkert og utilgjengelig for uvedkommende*
- *Vi utveksler ikke personopplysninger med tredjepart dersom dette ikke klart fremkommer av vår avtale med deg*
- *Dine reisedata vil alltid anonymiseres før de brukes til statistikkformål*
- *Det er frivillig å gi oss samtykke til behandling av personopplysninger. Dersom du ikke ønsker å gi oss slikt samtykke, skal vi tilby deg et anonymt alternativ"*

Under denne listen er det en lenke til skjemaet "behandling av personopplysninger"<sup>225</sup>. Skjemaet er et PDF-dokument som kan lastes ned.

Det nedlastbare skjemaet består av omtrent halvannen side tekst. Innledningsvis er en gjentakelse av anbefalingen om å registrere kortet. Denne teksten er identisk med annen tekst på nettsiden. Omtrent halvveis ned på første side står det om behandling av personopplysninger. Det opplyses om at behandlingen er nødvendig "for å gjøre din reise og kundeopplevelse så enkel og brukervennlig som mulig". Videre gis det en del eksempler på forskjellige typer personopplysninger. Det skilles mellom "reisedata" og "kundeopplysninger". Eksempelene på personopplysninger fremstår ikke som en utførmelig oversikt. Mer spesifikt nevnes gjennomføring av reiser, refusjon av billett og håndtere betaling og fakturainformasjon som mulige formål for behandlingen. Det presiseres at opplysningene ikke vil bli brukt til markedsføringsformål.

Om man velger "Ofte stilte spørsmål" fra forsiden på nettsiden (understreket med rødt i Bilde A) blir man sendt til en standard FAQ<sup>226</sup> av typen som ikke har mulighet for innsending av egne spørsmål.

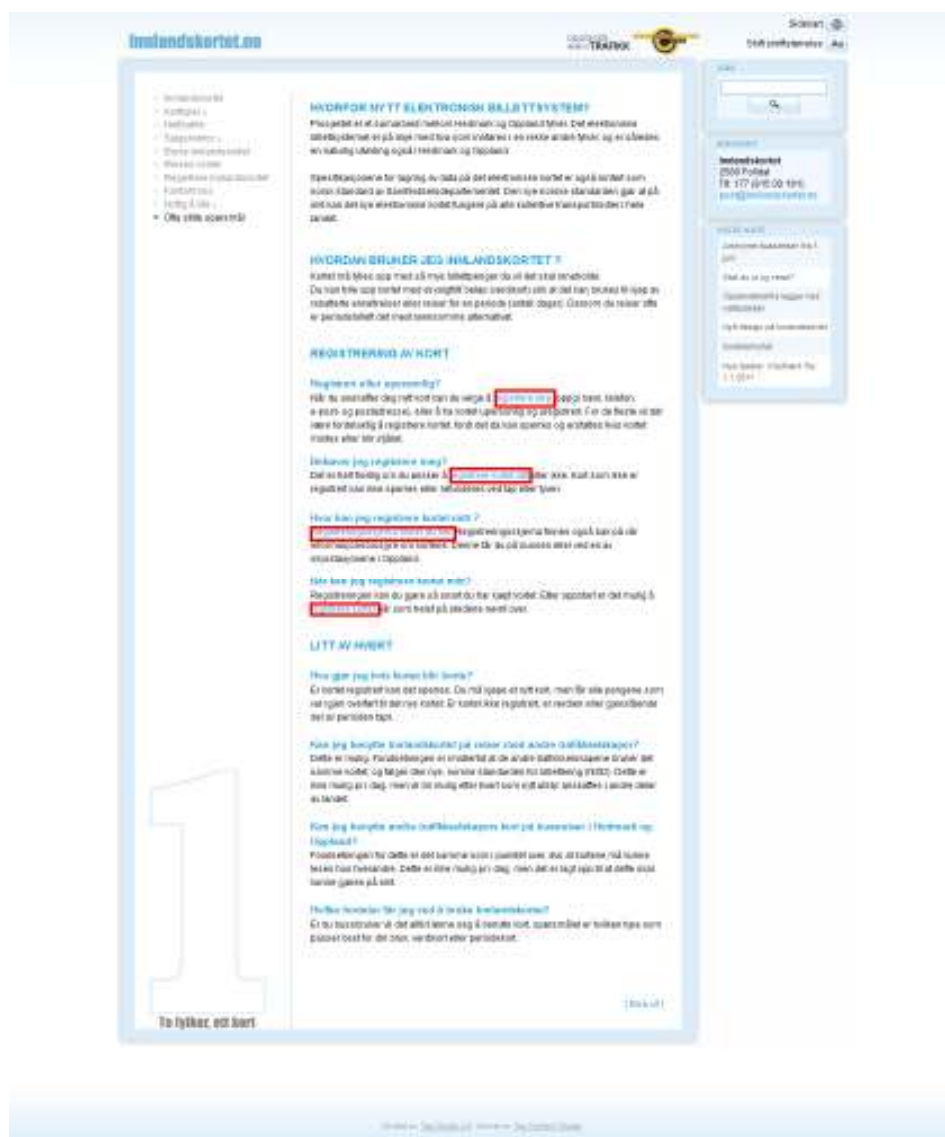
---

<sup>225</sup> Innlandskortets hjemmesider, *PDF om personvern* (2012).

<sup>226</sup> FAQ betyr Frequently Asked Questions og er vanlig å ha på nettsider.



Bilde C



Etter svar på spørsmål om hvorfor Innlandskortet i sin tid ble innført og hvordan det brukes, er det fire spørsmål knyttet til registreringen av kortet. De fire røde firkantene i Bilde C er alle lenker til nettsiden som inneholder registreringsrutinen. Det informeres om at registreringsprosessen krever at man oppgir navn, adresse, telefonnummer og e-postadresse og at det er frivillig å registrere seg. Utover dette er det ingen informasjon om personvern på denne siden. På alle punktene står det om fordelene ved å registrere seg.

## 5.2 Registreringsprosessen på nett

I mine intervjuer med representanter for HT og OT kom det frem at det ble vurdert å slutte med registrerte billetter hos Innlandskortet. Dette var da under vurdering. I løpet av mai måned stengte registreringsrutinen på nett. Dermed har det ikke vært mulig for meg å vurdere annet enn selve nettsiden og hvilken informasjon som gis frem til registreringsprosessen starter.

Fra forsiden er det lenket direkte til registreringssiden.<sup>227</sup> Selve registreringssiden inneholder en kort tekst og et skjema som må fylles ut. Teksten forklarer noen av fordelene ved registrering og informerer om at man kan få informasjon om produktet tilsendt. Det informeres ikke om hvordan man kan be om denne informasjonen, men i margen til høyre på siden finnes det generell kontaktinfo.

Selve skjemaet er om følgende opplysninger: Navn, adresse, postnummer, poststed, telefonnummer, fødselsdato, e-post og kortnummer. I tillegg blir man bedt om å presisere korttype og hvorvidt man ønsker å motta informasjon om Innlandskortet på e-post. Sistnevnte i form av en "checkboks" som allerede er markert med haketegn før utfyllingen starter.

Siden inneholder ingen informasjon om personvern eller lenke til slike sider. Verken i faste menyer i nettsidens "ramme" eller på selve siden. De tidligere omtalte faste menyene er selvsagt til stede, men ingen av knappene her går direkte til informasjon om personvern.

### 5.3 Andre kilder til informasjon

Bjørn Rune Holmen er teamleder IKT hos Oppland Trafikk og forteller i intervjuet at nettsidene deres er primærkilden til informasjon for kundene. Dersom det kommer informasjon gjennom andre kanaler, er det heller unntaksvis. Helge Olsen Bye, IT-medarbeider hos Hedmark Trafikk, forteller at sjåførene deres skal kunne svare på spørsmål om personopplysninger og personvern, men at det sjelden er henvendelser. Holmen forklarer også at HT og OT fortsatt har papirbilletter, men at for å få rabatter<sup>228</sup>, må man ha elektroniske billetter. Det er mulig å ha anonyme elektroniske billetter.

Som jeg har vært inne på tidligere, planlegger Innlandskortet å slutte med registrerte elektroniske billetter. De anser rekonstruksjon av tapte kort som den viktigste tilleggstjenesten til kundene. I fremtiden vil dette bli mulig dersom man kan fremvis kvittering på kjøpt billett, også med anonyme kort.

Olsen Bye fortalte meg at informasjonen også brukes til feilsøking i datasystemet og statistiske formål. Statistikken lages av anonymiserte reisedata. Olsen Bye forklarer også at de har en meget streng praksis på utlevering av reisedata til kunder som henvender seg. De må legitimere seg for å få innsyn. Han forteller også at det er mulig å trekke tilbake et samtykke ved å kontakte kundeservice. Koblingen mellom kort og identitet vil da slettes.

### 5.4 Drøftelse av innlandskortets praksis

Fra selve forsiden er det ingen direkte lenke til informasjon om personvernrelaterte spørsmål. Dersom man er aktivt på utkikk etter informasjon av denne typen, vil det

---

<sup>227</sup> Se rød firkant markert på Bilde A.

<sup>228</sup> For eksempel honnørrabatt eller studentrabatt.

være naturlig å gå til "ofte stilte spørsmål". Her er informasjonen sparsommelig og det henvises ikke videre til siden som omhandler personvern. Dersom man klikker på "registrer reisekortet" vil man ikke få noen info om konsekvensene av registreringen, kun mulighet til å fylle ut selve registreringsskjemaet. Det er ingen personvernrelatert informasjon tilgjengelig fra forsiden som er egnet til å informere brukeren om noe hun ikke selv aktivt ser etter. Eneste måten å komme til nettsiden om personvern, er å trykke "nyttig å vite". I nettsidens faste meny fremstår denne kategorien som en av de siste kategoriene det ville være naturlig å finne opplysninger om registrering av kort, personvern eller behandling av personopplysninger. Det er ikke det at informasjonen ikke er tilgjengelig, men det vil sannsynligvis kreve en systematisk gjennomgang av mesteparten av nettsiden for å finne den. En omstrukturering av menyen, navneendring på kategoriene eller en egen personvernkategori ville hjulpet veldig. At den mest sentrale informasjonen befinner seg på et nedlastbart PDF-dokument bidrar til å heve terskelen for å tilegne seg informasjonen ytterligere.

Om brukeren finner nettsiden om personvern, er informasjonen bedre. Det er allikevel slik at man må lese mesteparten av teksten før man blir får vite noe annet enn fordelene ved registrering. Det er positivt at personopplysningsloven nevnes ettersom dette gjør brukeren i stand til å vite hvor hun kan se etter det rettslige grunnlaget. Det presiseres at Innlandskortet trenger ditt samtykke og nevnes spesielt at anonyme reiser er en mulighet. Språket er lettlest og tydelig, men bærer preg av veldig mye gjentakelser. Det er kun informasjon om fordeler, ikke rettigheter eller personopplysninger, som er gjenstand for gjentakelse. Dette gjør det noe utfordrende å finne relevant informasjon i teksten. Den nedlastbare PDFen inneholder nok mest informasjon. Dessverre bærer teksten preg av å være kopiert fra Opplands Trafikks nettsider eller annen tilgjengelig informasjon ettersom det konsekvent skrives om OT som behandlingsansvarlig. Hedmark Trafikks logo er på brevhodet og de er også nevnt i teksten, men kun sporadisk og ikke konsekvent slik OT er. Dette bidrar ikke til tydelighet, men vil neppe føre til store misforståelser da Innlandskortet også brukes hyppig.

I punktlisten jeg har sitert i kapittel 5.1 forsikres det om at personvern tas seriøst, men den inneholder lite som kan hjelpe den registrerte å hevde egne rettigheter. Mye av informasjonen er lite konkret og på de områdene den er konkret, for eksempel om statistikk, sies det mest om hva opplysningene ikke brukes til. Det at ordlyden gir inntrykk av å være forsikringer om at "alt er bra" snarere enn å informere, kombinert med at PDFen ser ut til å være klipp og limt sammen av tidligere tekster gir et noe useriøst preg. Det er neppe avgjørende i en vurdering av hvorvidt informasjonen er tilstrekkelig, men kan bidra til å skape usikkerhet hos leseren.

Som jeg har nevnt tidligere, har jeg ikke klart å finne noe formål som er meldt til Datatilsynet, men i dokumentet<sup>229</sup> informeres det om formål. Det er uklart om dette er uttømmende eller ikke. Innlandskortet har ingen personvernombud registrert på

---

<sup>229</sup> Altså den nedlastbare PDFen.

datatilsynets nettsider.<sup>230</sup> Formålene som nevnes er etter mitt skjønn saklig begrunnet i bedriftens virksomhet. Det presiseres også at man må gi spesiell tillatelse til å bruke opplysningene i markedsføringsformål. Hva disse markedsføringsformålene er, spesifiseres ikke. I registreringsprosessen er det mulig å takke ja til å få informasjon tilsendt på e-post, så det er mulig det er dette som er "markedsføringsformål".

Det nevnes ikke utlevering til andre aktører, men presiseres at kundesentrene deres trenger tilgang til opplysningene for å håndtere blant annet innbetalinger. Det påpekes også at dersom man bruker Innlandskortet hos et annet selskap som godtar dette, vil opplysningene også utveksles med dette selskapet. Jeg tolker denne formuleringen dit hen at den opprinnelig er skrevet for å gjelde kun OT og dermed primært er ment for å beskrive eventuell bruk på rutene til HT. Dermed er det altså informert om utveksling mellom selskapene, dog på en noe utydelig måte. Dette bekreftes også av Helge Olsen Bye. Han forklarer at reisedata som genereres i et annet fylke enn der billetten er kjøpt, blir gjort tilgjengelig for begge selskaper i anonymisert form. Disse opplysningene brukes til avregning mellom selskapene.

Frivilligheten nevnes kun to steder på nettsidene. Det er siste punkt på personvernsiden før lenken til det nedlastbare dokumentet og i en bisetning om innsyn i og retting av opplysninger i selve dokumentet. Nederst på nettsiden om personvern informeres det også om at foreldre må samtykke for barn under 16 år.

Det informeres ikke om hvorvidt opplysninger slettes eller ikke. De eneste stedene det står om sletting er som en konsekvens av tilbaketrukket samtykke og i forbindelse med en beskrivelse av hvordan trafikk i nettbutikken lagres<sup>231</sup>. Begge disse avsnittene befinner seg i det nedlastbare dokumentet. På nettsiden om personvern informeres det om at informasjon som brukes til statistiske formål vil anonymiseres.

Så vidt jeg kan se er alle billettyper tilgjengelig også som uregistrerte. Nettsiden opplyser om betingelser for å få rabatter, men dette er altså forskjellen på papirbillett og elektronisk billett. Anonyme elektroniske løsninger gir det samme tilbudet med unntak av enkelte tilleggstjenester. Innlandskortet tilbyr også refusjon av tapt kort dersom du fremviser kvittering.

Ettersom registreringsprosessen ble stengt før jeg klarte å sikre skjermdump, er det ikke mulig for meg å vurdere hvorvidt den registrerte blir informert underveis i registreringsprosessen. For at et samtykke skal være tilstrekkelig informert, må imidlertid informasjonen gis i forkant av at samtykket inngås og før personopplysninger gis til behandlingsansvarlig. Derfor er det fortsatt relevant å se på den delen av prosessen som fortsatt er synlig, altså frem til og med utfylling av registreringsskjema. For en kunde som besøker innlandskortet.no er det ingen informasjon om personvern, behandling av personopplysninger eller hennes

---

<sup>230</sup> Datatilsynet, *Alfabetisk oversikt over personvernombudene* (2011).

<sup>231</sup> Blant annet gjennom såkalte "cookies".

rettigheter i løpet av det som må anses som den naturlige veien til registreringsskjemaet. Med naturlig vei, mener jeg den serien med lenker og nettsider som designet på nettsiden selv legger opp til, og som også er raskeste<sup>232</sup> vei til registreringssiden.

Selve registreringssiden inneholder som nevnt ingen informasjon som kan sørge for at et eventuelt samtykke er informert. Det informeres heller ikke om hvorvidt registreringen er frivillig, men det er heller ingen ting på siden som tilsier at dette er noe man må gjøre. Ordet samtykke er ikke nevnt et eneste sted på registreringssiden, det er ikke lenket videre til ytterligere informasjon. Det er heller ingen knapp som kan tilsa at dette er en erklæring fra den registrerte. Utover rent praktisk informasjon står det at "det lønner seg å registrere det nye kortet ditt".

Det er mulig det kommer mer informasjon senere i prosessen, men slik nettsiden er lagt opp, ville man måtte gi fra seg opplysninger før man får muligheten til å samtykke til at disse opplysningene kan behandles. Dette er forutsatt at det gis informasjon på et senere punkt i prosessen. I motsatt fall vil det også fremstå som uklart at man ved å gå videre i prosessen avgir samtykke.

Det er neppe gitt tilstrekkelig informasjon i forkant av prosessen til å hevde at et samtykke vil være informert. Det er heller ikke noe som gir grunnlag for å hevde at samtykket er en uttrykkelig erklæring fra den registrerte. Dette fremstår som en del av en prosess for å få registrert innlandskortet og høste fordelene som følger av dem, snarere enn noe som har med utlevering av personopplysninger å gjøre. Det eneste som kan sies å ligne på en uttrykkelig erklæring er punktet der man kan hake av for å motta informasjon på e-post. Som jeg har vært inne på tidligere er det muligens dette som er markedsføringsformålene som nevnes et annet sted på siden. Denne haken er som standard huket av og krever ingen innsats eller aktiv handling fra den registrerte for å godkjennes sammen med registreringsskjemaet.

Uansett hvor man beveger seg på nettsidene er kontaktinformasjon til kundesenteret godt synlig i margin til høyre. Både postadresse, telefonnummer og e-postadresse. I det nedlastbare dokumentet informeres det om den registrertes rett til innsyn og mulighet til å få rettet opplysninger. Her nevnes også tilbaketrekking av samtykke som forutsetter innlevering av Innlandskortet. Slik teksten fremstår, ser dette ut til å være den eneste muligheten til å få opplysninger slettet.

Totalinntrykket av nettsiden er at informasjonen kun vil leses dersom brukeren leter etter den. Mesteparten av informasjonen er snarere reklame for registrering enn informasjon om behandling av personopplysninger. Den informasjonen som anses som relevant bærer noe preg av å være ufullstendig og generell. Så vidt jeg kan se er det kun to avsnitt som konkret sier noe om typer personopplysninger og bruk av Innlandskortet. Den øvrige informasjonen er av en generisk art at den kunne omtalt

---

<sup>232</sup> Færrest mulige klikk.

behandling av personopplysninger på en hvilken som helst nettside for et hvilket som helst firma.

## 5.5 Oppsummering

Som i kapittel 4.5 har jeg også her forsøkt å gi kravene fra drøftelsen i kapittel 3 "karakter". Under tabellen vil jeg også her kort oppsummere totalinntrykket.

Krav	Oppfylt
Er informasjonen tydelig og lett å finne?	1
Er informasjonen entydig?	1
Er språket lett forståelig?	2
Er formål formulert på forhånd?	0
Er formål kommunisert til den registrerte?	1
Er formål saklig begrunnet i bedriftens virksomhet?	2
Er det informasjon om hvorvidt opplysningene blir utlevert til andre?	2
Er det informasjon om hvorvidt det er frivillig å gi fra seg opplysningene?	1
Informeres det om samtykkets varighet?	1
Informeres det om lagringstid før opplysningene slettes?	0
Er det informasjon om hvorvidt opplysninger anonymiseres?	2
Er det anonyme alternativer tilsvarende registrert billett tilgjengelig?	2
Er relevant informasjon gitt før den registrerte gir fra seg opplysninger?	0
Krever samtykket en aktiv handling, eller er den innebygget i en annen prosess?	0
Er kontaktinfo til behandlingsansvarlig lett tilgjengelig?	2
Er det lagt til rette for innsyn?	2
Er det muligheter for å rette informasjon?	2
Er det lagt til rette for å kunne trekke tilbake samtykke?	1
Er det mulig å få opplysningene slettet?	1

Heller ikke Innlandskortet klarer "godkjent" på alle punkter. Nettsidene er preget av et lett forsåtelig språk uten bruk av bransjespesifikke eller juridiske faguttrykk. Også her er informasjonen krystallklar på enkelte områder, men også denne nettsiden ser ut til

å forsøke å "gjemme" personvernrelatert informasjon bak fordelene ved å registrere seg. Totalinntrykket er nok at dette i større grad er tilfellet på denne siden enn hos Ruter. Informasjonen er også noe vanskeligere tilgjengelig, men til gjengjeld er den samlet på færre sider. Igjen aktualiseres dilemmaet mellom selskapets interesse i presenteres praksisen sin som tiltalende og informasjonsplikten. Jeg skal innrømme at jeg er usikker på om fakta om personvern og behandling av personopplysninger er presentert på en slik måte at den gir tilstrekkelig informasjon til leseren. Jeg har under sterk tvil valgt å gi de to første punktene i kravlisten karakteren 1. La meg understreke at det ikke er noe i veien med språkets tydelighet. Det er først og fremst hvor vanskelig det er å finne personverninformasjon, samt måten all relevant informasjon presenteres mellom store mengder "reklametekst".

Jeg har valgt å gi Innlandskortet en "0" i spørsmålet om formålet er formulert på forhånd. De har verken registrert melding hos Datatilsynets meldingsdatabase eller eget personvernombud. Dette fremstår først og fremst som en glemt formalitet, ettersom det nedlastbare dokumentet er tydelig, både på hva opplysningene skal brukes til og ikke brukes til. Forbedringspotensialet her ligger i å formulere det på en måte som fremstår som uttømmende.

Heller ikke her presiseres det om samtykkets varighet, men det informeres om muligheten til å trekke det tilbake og dermed antydes det at samtykket i utgangspunktet er evigvarende. Det er ingen informasjon om hvor lenge opplysninger lagres.

De to siste punktene som har fått karakter "0" er meget sentrale for om samtykket kan anses som gyldig eller ikke. Det er mulig å gå gjennom registreringsprosessen uten å bli utsatt for ordet samtykke en eneste gang. Det er heller ingen informasjon om frivillighet. Den eneste aktive handlingen det er mulig å gjøre er å sende inn et skjema som tilsynelatende ikke har noe med å gi et samtykke å gjøre. Den eneste muligheten man har til å justere hva man godtar er å velge om man vil ha tilsendt tilbud på e-post eller ikke. Heller ikke dette er noe man må velge, det er ferdig valgt for kunden når hun kommer til registreringsskjemaet.

Et utfylt registreringsskjema på denne nettsiden tilfredsstiller ikke de rettslige kravene til et samtykke. Innlandskortets sider er gode på informasjonen som er knyttet til innsyn, retting og sletting, samt hva opplysningene brukes til, hvem som har tilgang til dem og anonymisering i forbindelse med statistikk. Om Innlandskortet skulle ønske å satse på registrert kort igjen, vil dette etter mitt skjønn kreve en omlegging av strukturen på deler av nettsiden.

## 6.0 Bransjenormen

Jeg har nå langt på vei svart på spørsmålene i problemstillingen min, men det er et regelsett jeg enda ikke har sett på. *Bransjenorm for personvern og informasjonssikkerhet i elektronisk billettering* er utarbeidet som et samarbeid mellom Datatilsynet og en rekke aktører i bransjen. Bransjenormen ble ferdigstilt mens denne

oppgaven ble skrevet og trer i kraft juni 2012. Bransjenormens juridiske status er noe uklar. Bransjenormen er hjemlet til personopplysningsloven som oppfordrer til utviklingen av "bransjevisse adferdsnormer" der dette lar seg gjøre.<sup>233</sup> Slike normer vil trolig være veiledende i utgangspunktet, men selv om Bransjenormen ikke kan regnes som rettskilde på lik linje med en forskrift er den fortsatt bindende for de aller fleste tilbydere av kollektivtransport i landet. I følge Bransjenormens kapittel 2 er "alle virksomheter som har løyve eller mottar tilskudd [...] forpliktet til å følge Håndbok 206"<sup>234</sup>. Håndbok 206<sup>235</sup> skal også henvise til Bransjenormen,<sup>236</sup> noe som gjør den bindende for aktørene. Det er også mulig for virksomheter som ikke er bundet av Håndbok 206 å slutte seg til Bransjenormen. Selv om Bransjenormen er bindende for de fleste kollektivselskaper i Norge, er den ikke uttømmende. Det er med andre ord rom for at det stilles tilleggskrav til aktørene i bransjen i for eksempel lov og forskrift. Slik jeg har forstått det, vil Bransjenormen være malen når Datatilsynet i fremtiden gjør kontroller hos kollektivselskapene. Bransjenormen kan dermed ende opp med å bli definerende for kollektivselskapenes praksis i større grad enn lov og forskrift er i dag. Samtidig er det viktig å huske på noe Atle Årnes fra Datatilsynet påpekte under intervjuet, nemlig at man kan bli enige med bransjen om retningslinjer, men ikke utenfor de rammene loven setter.

Selv om Bransjenormen ikke er nødvendig for å utrede gjeldende rett i snever forstand, vil normen bli obligatorisk og dermed bli potensielt avgjørende for hvordan loven praktiseres. Jeg vil først ta en gjennomgang av reglene som går på samtykke og frivillighet. Deretter vil jeg se på de regler som handler om kundens mulighet til innsyn, retting og sletting før jeg går over til de øvrige reglene i normen. Avslutningsvis vil jeg se på hva casene mine eventuelt må gjøre for å tilfredsstille Bransjenormens krav når den trer i kraft.

## 6.1 Generelt om Bransjenormen

Bransjenormen består av 12 kapitler fordelt på 18 sider og kan blant annet finnes på datatilsynets hjemmesider. Normens utgangspunkt er at det er en "politisk målsetting" å implementere løsninger for elektronisk billettering i Norge og at Bransjenormen skal kunne sørge for "forutsigbarhet for aktørene" når de må forholde seg til lovverket og sikre personvernet til de reisende.<sup>237</sup>

Bransjenormen henviser til 5 vedlegg med tilleggsopplysninger. Disse er dessverre ikke offentliggjort. I intervjuet med Wandaas fikk jeg inntrykk av at vedleggene ikke var vedtatt og dermed ikke trådt i kraft. Atle Årnes hos Datatilsynet virket overrasket over at vedleggene ikke lå tilgjengelig på nett, men ønsket ikke å utlevere disse før han hadde dobbeltsjekket med de andre aktørene at det var enighet rundt disse.

---

<sup>233</sup> Jfr. Ot. Prp. Nr. 92 (1998-99), Kapittel 6.10.

<sup>234</sup> Bransjenormen, s. 1.

<sup>235</sup> *Håndbok 206 Elektronisk billettering*(2011).

<sup>236</sup> Jeg har ikke funnet denne henvisningen i de delene av håndboken som ligger offentlig ute på vegvesenets nettsider.

<sup>237</sup> Bransjenormen, s. 1.



Ingen av aktørene jeg har snakket med har ønsket å gi meg tilgang til disse vedleggene utover en kort beskrivelse av deler av innholdet.

Bransjenormen plasserer behandlingsansvaret hos øverste leder i virksomheten.<sup>238</sup>

## 6.2 Samtykke og frivillighet i Bransjenormen

I Bransjenormens kapittel 5 slås det fast at man som reisende "har en grunnleggende rett til å kunne bestemme over sine personopplysninger og til å kunne velge å ferdes anonymt i samfunnet."<sup>239</sup> Videre sies det at det å ferdes anonymt er "en viktig del av privatlivet".

Det stilles krav til at behandling av personopplysninger skal baseres på samtykke og understrekes at samtykket kun er frivillig dersom det finnes reelle anonyme alternativer til de registrerte billettene. Frivilligheten forutsetter at det anonyme alternativet koster det samme eller mindre enn det registrerte. Tilbudene kan variere på innhold, men ikke i pris. Bransjenormen definerer anonyme kort som "kort som virksomheten ikke kan knytte til en person"<sup>240</sup>, men hevder samtidig at det er tilstrekkelig at kortet ikke er registrert på innehavers navn hos kollektivselskapet for at dette kravet er oppfylt<sup>241</sup>.

Det gjøres unntak fra samtykke som behandlingsgrunnlag ved billettkontroll og i forbindelse med Skoleskyss.<sup>242</sup> Behandlingsgrunnlagene for disse formålene er henholdsvis "berettiget interesse" og "å utøve offentlig myndighet".<sup>243</sup> Det nevnes også eksplisitt at det er relevant å behandle fødselsnummer for å administrere skoleskyss.<sup>244</sup>

Kjøp av billetter skal kunne gjøres anonymt og det samme gjelder refusjon og rekonstruksjon av tapte kort "så langt som mulig"<sup>245</sup>. Det er uklart hvor vanskelig dette må være å gjennomføre for at det ikke lenger anses som mulig.

Bransjenormen stiller formkrav til samtykke og er dermed mer spesifikk enn lovverket. Muntlig samtykke godkjennes, men det anbefales å benytte seg av en eller annen form for skriftlighet av hensyn til etterprøvbareheten.<sup>246</sup> I "vedlegg 2" til Bransjenormen er det en mal for hvordan man kan formidle informasjonen i forkant av et samtykke. Som tidligere nevnt er ikke vedleggene tilgjengelige, så det er ikke mulig for meg å vurdere denne malen.

---

<sup>238</sup> Bransjenormen, s. 12.

<sup>239</sup> Bransjenormen, s. 3.

<sup>240</sup> Bransjenormen, s. 16.

<sup>241</sup> Bransjenormen, s. 3.

<sup>242</sup> Henholdsvis kapittel 7.1.4 og 7.1.5, begge i Bransjenormens s. 8.

<sup>243</sup> Jfr. popplyl § 8 bokstav f og e.

<sup>244</sup> Bransjenormen, s. 9.

<sup>245</sup> Bransjenormen, s. 4.

<sup>246</sup> Bransjenormen, s. 6.

Ifølge Bransjenormen skal samtykkeerklæringen og informasjonen i forkant som et minimum inneholde informasjon om:

- at samtykket er frivillig
- at anonyme alternativer eksisterer
- hva som er formålet med behandlingen
- hvor opplysninger eventuelt utleveres
- detaljert beskrivelse av hva som samles inn
- beskrivelse av hvordan man kan be om innsyn, retting og sletting av feil informasjon
- hvem som er behandlingsansvarlig

Dersom det finnes anonymiserte innloggingsløsninger på nett, skal det ikke være mulig å fylle inn ekstra eller overflødige opplysninger da dette kan bidra til identifisering. For eksempel ved at det står tomme felter hvor dette er mulig på profilsiden.<sup>247</sup>

### 6.3 Innsyn, sletting og retting i Bransjenormen

Bransjenormen skiller mellom generell innsynsrett (kapittel 6.1) og registrerte kunders innsynsrett (kapittel 6.2). Den generelle innsynsretten gjelder informasjon om behandlingsansvarlig, formålet med behandlingen, hvor opplysningene er hentet fra og hvorvidt de vil bli utlevert til andre. Det presiseres at den generelle innsynsretten "omfatter ikke innsyn i Reiseopplysninger". Reiseopplysninger er definert som "opplysninger fra en transaksjon på Kortet som registreres ved bruken av en Billett."<sup>248</sup> Likevel skal uregistrerte kunder få innsyn i slike opplysninger dersom det er for å sikre at billetten fungerer som den skal. For eksempel ved en klage på belastning av kortet. I et slikt tilfelle vil det være naturlig å fremvise kortet.

En slik løsning gir innehaveren av et uregistrert kort få muligheter til å undersøke hva som er lagret om ens eget kort, men vil samtidig styrke den enkeltes personvern ved at misbruk bli mer usannsynlig. Det fører også til en ytterligere distanse mellom reiseopplysningene og kundens identitet og underbygger på sett og vis påstanden om at uregistrerte kort er anonyme.

I tillegg til dette har registrerte kunder krav til innsyn i alle "opplysninger registrert om seg selv"<sup>249</sup>. Det gjøres et skille mellom betaler og den registrerte. Skillet kan sammenlignes med skillet mellom juridisk eier og bruker av et telefonnummer som finnes hos mobiloperatører. Det er kun den registrerte/brukeren som har krav på innsyn i detaljerte reiseopplysninger. Den registrerte har også krav på informasjon om sikkerhetstiltakene rundt behandlingen av opplysningene. Kort oppsummert kan

---

<sup>247</sup> Bransjenormen, s. 12.

<sup>248</sup> Bransjenormen, s. 16.

<sup>249</sup> Bransjenormen, s. 4.

man si at den registrerte innsynsrett består av det mer eller mindre det samme som er beskrevet i popplyl §§ 18 og 19.

Ved innsynsforespørsler forplikter virksomheten å forsikre seg om at det kun er den registrerte som mottar opplysningene.<sup>250</sup> Bransjenormen tillater ikke at svar på innsynsforespørsler sendes per e-post. Tidsfristen følger personopplysningslovens standard på senest 30 dager og uten ugrunnet opphold.<sup>251</sup>

Dersom det utleveres opplysninger til andre enn den registrerte skal den registrerte alltid informeres om hva, til hvem og hvorfor.

Sletting skal, i tråd med personopplysningsloven,<sup>252</sup> skje så snart opplysninger ikke lenger er nødvendige. Alle reiseopplysninger skal slettes etter 104 dager. Kundeopplysninger, som for eksempel kontaktinformasjon, skal "slettes senest 14 dager etter avtaleforholdet er avsluttet"<sup>253</sup>. Det henvises til egne regler i Vedlegg 5 for opplysninger som gjelder fakturering eller arkivering. Dette vedlegget er ikke opprettet enda.

#### 6.4 Øvrige bestemmelser i Bransjenormen

Bransjenormen har en egen bestemmelse for bruk av personprofiler. Det skal gis et selvstendig samtykke for at virksomheten skal kunne gi kundene skreddersydde tilbud basert på bruk og preferanser. Det finnes en mal for hvordan et slikt samtykke kan innhentes i vedlegg 2. Utover dette er det ingen beskrivelse av hva en personprofil er for noe, men det er nærliggende å tro at begrepet samsvarer med personprofiler som beskrevet i popplyl § 21.

Det er tillatt å drive med direkte markedsføring ovenfor kunden, men kunden skal gis mulighet til å reservere seg ved enhver henvendelse på en enkel måte.<sup>254</sup>

Videre er det bestemmelser om formål som samsvarer godt med personopplysningsloven.<sup>255</sup> Opplysninger skal ikke brukes til andre formål enn de er samlet inn for, formål skal begrunnes saklig i bedriftens virksomhet og opplysningene som samles inn må være relevante for å oppnå formålet. Det opplyses om at det i Vedlegg 1 er en del eksempler på sammenhengen mellom formål og relevante opplysninger.

Virksomhetene skal utvikle rutiner for sine plikter og dokumentere disse. For eksempel rutiner for raskt innsyn og sletting av unødige opplysninger. Det skal også sikres at kun de ansatte som har behov for det, har tilgang til personopplysninger. Det skal logges hvem som gjør oppslag opp i disse. Følgelig skal det mellom

---

<sup>250</sup> Bransjenormen, s. 5.

<sup>251</sup> Jfr. popplyl § 16.

<sup>252</sup> Jfr. popplyl § 28.

<sup>253</sup> Bransjenormen, s. 9.

<sup>254</sup> Bransjenormen, s. 7.

<sup>255</sup> Bransjenormen, s. 8.

selskaper tilhørende samme billettsystem kun utveksles de opplysninger som er absolutt nødvendig for avregning selskapene imellom. Bransjenormen anbefaler virksomhetene å opprette personvernombud.

I kapittel 10 finnes det rutiner for hvordan revidering av Bransjenormen skal gjennomgå, samt hvem en eventuell arbeidsgruppe som gjør dette arbeidet skal bestå av. Enhver bruk av ny teknologi, for eksempel "mobiltelefoner som billettbærere", skal godkjennes i henhold til reglene i kapittel 10.<sup>256</sup>

Videre følger en rekke tekniske detaljer som skal sikre anonymitet gjennom nettløsninger og unngå unødig logging av IP-adresser og lignende.

I tillegg er det enkelte regler som krever at det skal gjøres risikovurderinger, registreres avvik og at virksomhetene skal etablere rutiner for internkontroll med mer. Jeg skal ikke gå videre inn på disse bestemmelsene, da det er litt på siden av det jeg ser på i denne oppgaven utover å nevne at de grovt sett samsvarer med popplyl §§ 12-15.

## 6.5 Oppsummering av Bransjenormen

At bestemmelsene i Bransjenormen automatisk gjelder de fleste kollektivselskaper i landet er et stort skritt i retning av en standardisering. Dette vil også kunne føre til at leverandørene av IT-løsninger på området må tilpasse seg. I mitt intervju med Bjørn Rune Holmen ble det uttrykt at flere av avvikene Datatilsynet hadde pekt på, spesielt det som handlet om unødig lagring av data, var et resultat av oppbygningen av datasystemet levert av Fara AS. Mange av systemets funksjoner og hvilke opplysninger som ble lagret var ukjente for de som jobbet hos HT og OT frem til Datatilsynets kontroll. Dersom leverandørene må tilpasse seg Bransjenormens krav, vil dette kunne få store positive konsekvenser for korrekt lagring, sikring og sletting av opplysninger fremover. En felles bransjenorm vil forhåpentligvis også gjøre møtet med billettsystemer mer forutsigbart for kundene.

Bransjenormen påvirkningskraft er avhengig av at den gjøres kjent, gjerne for kunder/brukere, men først og fremst for kollektivtransportprodusentene. At Bransjenormen oppfordrer til bruk av personvernombud vil også kunne øke kunnskapen hos kollektivselskapene. Jeg tror et slikt ombud forankrer kunnskap om personvernet i den enkelte bedrift i mye større grad enn et regelsett vil gjøre. Samtidig er det en stor ulempe at vedleggene ikke er tilgjengelige offentlig, da store deler av teksten henviser til disse, samt at eksempler som kan være et godt utgangspunkt for etterlevelse av punktene befinner seg i vedleggene. Mitt inntrykk er at aktørene som har vært med å utvikle normen ønsker at disse skal vedtas, og trolig vil vedleggene blir allment tilgjengelige etter hvert.

Bransjenormen er krystallklar på behandlingsgrunnlagene og går også langt i å avgrense deler av de tekniske løsningene som kan tas i bruk. Reell frivillighet er også

---

<sup>256</sup> Jfr. kapittel 7.9. Bransjenormen, s. 11.

grundig drøftet. Normen er noe tilbakeholden med å stille formkrav til informasjonen i forkant av et samtykke. Kravene fokuserer hovedsakelig på innholdet fremfor form, plassering og synlighet. Det er neppe lurt å låse seg til en mal, da det sikkert finnes mange gode muligheter for formidling som ikke er tenkt på enda, men det kan også føre til at en del spørsmål forblir ubesvart. Spesielt med tanke på grensedragningen om hvor tydelig slik informasjon må presenteres.

Ellers er Bransjenormen langt på vei i tråd med mine egne vurderinger av lovverket. På enkelte områder mer konkret, mens andre områder er mer diffuse eller generelle. Sistnevnte er ofte de områder der loven er rimelig spesifikk og således kan det kanskje anses som overflødig å presisere dette i normen.

## **6.6 Reisekortet og Innlandskortet i lys av Bransjenormen.**

Som jeg har vært inne samsvarer Bransjenormen langt på vei med min egen punktliste som var utgangspunkt for vurderingene i kapittel 4 og 5. Jeg har muligens stilt mer konkrete krav til utformingen av informasjonen som gis i forkant av samtykke. Blant annet ved å se på språket på nettsidene. Dette er uansett områder begge casene klarte seg bra på. Jeg er usikker på om Bransjenormen bør tolkes dit hen at den i større grad krever at personvernrelatert informasjon skal presenteres for kunden i forkant av, eller som et ledd i, registreringsprosessen. Casene tilfredsstiller neppe dette kravet ettersom mesteparten av den relevante informasjonen hos begge caser befinner seg andre steder enn i selve registreringsprosessen. Dersom den døde lenken på ruter.no henviste korrekt, ville dette muligens tilfredsstilt et slikt krav. Det avgjørende er hvor spesifikt/detaljert en henvisning til slik informasjon må være. Holder det å henvise til vilkår for samtykke eller informasjon om personopplysninger, eller må kunden i større grad få detaljert informasjon om hva det henvises til?<sup>257</sup>

Bransjenormen krever meget detaljert informasjon om hva slags opplysninger som samles inn. Behandlingsansvarlig må for eksempel informere om detaljnivå på reiseopplysninger.<sup>258</sup> Ingen av casene tilfredsstiller kravet til et slikt detaljnivå.

Ruter tilbyr ikke anonym refusjon av tapte kort, og ingen av selskapene tilbyr anonym rekonstruksjon av tapte kort så vidt meg bekjent. Her må det nevnes at Bransjenormen kun krever dette "så langt det er mulig" uten å utdype hva dette vil si. Dermed blir det vanskelig å vurdere hvorvidt selskapene etterlever Bransjenormen på dette punktet i dag.

Bransjenormens generelle innsynsrett gir også eier av et anonymt ihendehaverkort en begrenset innsynsrett. Dette følger ikke av loven ettersom et anonymt kort ikke genererer personopplysninger. Trolig vil begge casene kunne håndtere slike henvendelser på samme måte som en tilsvarende henvendelse fra en registrert

---

<sup>257</sup> Det er mulig å tenke seg henvisninger av typen "for oversikt over hvilke opplysninger som behandles, trykk her" eller "Ved å gå videre, samtykker du til at vi kan bruke dine opplysninger til følgende formål".

<sup>258</sup> For eksempel presisere at det lagres holde plass, klokkeslett og transaksjoner på kortet.

kunde. Forskjellen er som nevnt at generell innsynsrett ikke gir tilgang på reiseopplysninger.

Ingen av casene mine har lagt opp til å skille mellom den registrerte og en eventuell betaler av kortet. Dette vil neppe bryte med kravene i Bransjenormen ettersom formålet med et slikt skille må være å sørge for at kun den registrerte får innsyn og det ser ut til å være tilfredsstilt.

Kravet til at man skal kunne reservere seg mot direkte markedsføring ved enhver henvendelse er jeg usikker på om er ivarettatt i dag. Ruter tilbyr ikke slik markedsføring og dermed er problemstillingen uaktuell. Innlandskortet har dette som et valg under registreringen. Uansett vil det trolig være tilstrekkelig med en tekst som informerer om muligheten for å reservere seg mot markedsføringen på alle utsendelser.

Normen inneholder også en del regler som er av mer IT-teknisk art. Blant annet at det skal logges hvem som gjør oppslag i personopplysninger. Om det er slik i dag, har jeg ikke mulighet til å vurdere. Jeg vil derfor nøye meg med å påpeke at hvorvidt dette er et enkelt krav å justere seg etter, er meget avhengig av programvaren til billettsystemet.

Slik jeg ser det blir kollektivselskapene nødt til å omstille seg noe for å kunne tilfredsstille Bransjenormens krav. Det avgjørende spørsmålet er hvor strengt kravet om å informere i forkant av samtykke skal tolkes. En veldig streng tolkning vil kreve relativt store omveltninger i strukturen på nettsidene. Dette for å gjøre det mulig å henvise til relevant informasjon på mer synlige steder eller mer synlige måter. Det vil trolig også kreve at selskapene i større grad blir nødt til å dele opp personvernrelatert tekst på nettsidene sine for å kunne porsjonere det ut,<sup>259</sup> snarere enn å henvise til en større tekst som inneholder all informasjon.

Jeg noterer meg også at Bransjenormen krever at enhver ny teknologi må godkjennes før den kan tas i bruk. Så vidt meg bekjent har NSB allerede åpnet for å bruke mobiltelefoner som billett bærer. Visstnok jobber Ruter med å utvikle en egen tilsvarende løsning.<sup>260</sup> Hvilke krav Bransjenormen vil stille til slike løsninger, vet vi ikke enda, men det er åpenbart at implementering ikke kan igangsettes uten videre.

---

<sup>259</sup> For eksempel ved å ha informasjon om frivillighet og samtykke ett sted og innsyn, retting og sletting et annet sted.

<sup>260</sup> Dette i følge Ruters egen twitterkonto: @ruter. <https://twitter.com/Ruter>

## 7.0 Oppsummering og samlede vurderinger

I denne oppgaven har jeg forsøkt å svare på følgende problemstilling:

- 1) *Hva brukes som behandlingsgrunnlag for opplysningene som samles inn?*
- 2) *Hvilke rettslige krav stilles til behandlingsgrunnlaget selskapene benytter seg av?*
- 3) *Hvordan er praksis for innsamling av personopplysninger og informasjon til de registrerte i selskapene?*
- 4) *I hvilken grad er praksis hos selskapene i tråd med de rettslige krav som stilles etter spørsmål 2?*

Jeg vil først gjennomgå problemstillingen og hvilke svar jeg har fått på spørsmålene den stiller. Deretter vil jeg se på hvilke utfordringer kollektivselskapene står ovenfor. Avslutningsvis vil jeg si noe om mulige løsninger på disse utfordringene og hvilken rolle Bransjenormen kan spille i forhold til disse.

### 7.1 Problemstillingen oppsummert

Jeg har tatt utgangspunkt i de to casene Reisekortet (Ruter) og Innlandskortet (Hedmark Trafikk og Oppland Trafikk) og sett på hvilket behandlingsgrunnlag disse benytter seg av for å behandle personopplysninger i forbindelse med elektroniske billettsystemer. Med unntak av det lovpålagte Skoleskysstilbudet og i forbindelse med billettkontroller, har begge selskaper opplyst at de benytter seg av samtykke som behandlingsgrunnlag.

I kapittel 3 har jeg først forsøkt å avklare når brukergenererte reiseopplysninger er for personopplysninger å regne. Jeg har konkludert med at hensiktsmessighetshensyn tilsier at uregistrerte ihendehaverkort ikke inneholder personopplysninger, men at ved en eventuell henvendelse fra kunden til behandlingsansvarlig, blir opplysningene knyttet til kortet å regne som personopplysninger så lenge de er sammenstilt. Videre har jeg sett nærmere på i hvilken grad andre behandlingsgrunnlag enn samtykke kunne vært benyttet og avklart samtykkets status i forhold til nødvendighetsgrunnene. Jeg har vist at samtykke er det eneste behandlingsgrunnlaget som kan brukes for å behandle personopplysninger fra registrerte kort.

Deretter har jeg tatt utgangspunkt i samtykkets definisjon, samt øvrige bestemmelser i personopplysningsloven og kommet frem til en punktliste med krav. Dette er krav jeg mener loven stiller til et kollektivselskap som skal benytte seg av registrerte kort. Punktlisten er begrenset til de områdene jeg har hatt mulighet til å undersøke gjennom observasjon og intervjuer. Den er med andre ord ikke uttømmende for alle kollektivselskaperes forpliktelser.<sup>261</sup> Denne punktlisten har vært utgangspunktet for mine vurderinger av kollektivselskapene i kapittel 4 og 5.

---

<sup>261</sup> Særlig forpliktelser av IT-teknisk art er blant forpliktelsene jeg ikke har sett på.

I kapittel 4 og 5 har jeg sett på selskapenes praksis knyttet til registrering av kort. Jeg har ikke kun sett på registreringsrutinene, men også hva resten av nettsiden inneholder. Nettsidene utgjør mesteparten av disse vurderingene i oppgaven og andre informasjonskilder har først og fremst bidratt å gi meg en forståelse av konteksten billettsystemene befinner seg i. En gjennomgang av registreringsrutinene på selskapenes nettsider viser at det neppe innhentes gyldig samtykke på noen av sidene. Det er riktignok varierende hva som mangler og varierende grad av tilpasning som skal til for at nettsidene skal tilfredsstillere lovens krav. Om man tar utgangspunkt i et personvernperspektiv er det relativt store rom for forbedringer. Brorparten av dette forbedringspotensialet er knyttet til hvordan det kommuniseres og hva som kommuniseres til kundene.

## 7.2 utfordringer i bransjen

Jeg har avdekket at casenes praksis ikke er i tråd med personopplysningsloven, men dette skyldes neppe ren vrangvilje fra kollektivselskapenes side. Da Datatilsynet gjorde kontroller på en rekke billettsystemer i 2009 og 2010 ble det avdekket feil hos samtlige som ble kontrollert. Det er grunn til å tro at etterlevelse av loven er en utfordring også hos andre aktører i bransjen. Jeg vil derfor trekke frem det jeg tror er to hovedgrunner til spriket mellom gjeldende rett og dagens praksis.

### 7.2.1 Lovtolkning

I løpet av arbeidet med denne oppgaven har jeg blitt nødt til å gjøre en rekke avveininger i tolkningsspørsmål.<sup>262</sup> Flere av avveiningene har vært svært vanskelige og litteratur på området har vært preget av generelle vurderinger. I enkelte tilfeller har jeg også forsøkt å drøfte disse tolkningene med forskjellige fagmiljøer uten å få klare svar. Særlig har spørsmålet om anonymitet ved bruk av ihendehaverkort vanskelig. Selv om det var enklere å vurdere hva et informert samtykke forutsetter, sier loven lite om hvilke krav som stilles til tilgjengeligheten og presentasjonen av relevant informasjon.

Trolig er dette en minst like stor utfordring for kollektivselskapene. Særlig for de mindre selskaper som har færre ressurser<sup>263</sup> å trekke på. Det ikke selvsagt at det er ansatt jurister hos alle kollektivselskaper, langt mindre en med særlig kunnskap om personopplysningsloven. I enkelte tilfeller vil det kanskje være IT-ansvarlig eller lignende som må ta avgjørelsene knyttet til dette. Det er ikke unaturlig at resultatet kan bli varierende og ofte vil det nok også være fristende å konkludere med at den enkleste løsningen er god nok.

I mange tilfeller vil en ansatt som utformer kravspesifikasjonen i praksis bli en lovanvender. Dette er problematisk dersom lovtolkningen er upresis. I enkelte tilfeller vil billettsystemene presenteres kollektivselskapet som en ferdig løsning fra en ekstern tilbyder. I slike situasjoner vil også de som utformer systemet potensielt ende

---

<sup>262</sup> Spesielt i utredningen i kapittel 3.

<sup>263</sup> Både menneskelige og økonomiske.



opp som lovanvendere. En risiko er at eksterne tilbydere er mer opptatt av å gi kunden<sup>264</sup> mest mulig valuta for pengene enn å tolke personopplysningsloven. I ytterste konsekvens vil dette kunne føre til at billettsystemene lagrer mer enn de trenger og dermed gir brukeren av systemet flere muligheter.

Denne utfordringen er beslektet med den andre mulige årsaken til at dagens praksis ikke alltid følger loven.

### 7.2.2 Utvikling av billettsystemene

I arbeidet med oppgaven har det blitt tydelig for meg hvordan en god prosess for bestilling og/eller utvikling av billettsystemet er viktig for personvernet.

En forutsetning for å utforme en god kravspesifikasjon, er å vite hva programmet skal kunne gjøre. Dette krever kunnskap om lovens krav til drift av systemet. Enten det er snakk om å utvikle programvare på egen hånd, eller bestille en ferdig løsning, er det en rekke tekniske muligheter som bør presiseres. Eksempler på dette kan være muligheten for å anonymisere opplysninger, muligheten for å ha anonyme kort eller logging av medarbeidere som gjør oppslag i opplysningene.

I intervjuet med Bjørn Rune Holmen (Oppland Trafikk) var det tydelig at datasystemet var designet på en slik måte at det ble lagret mer enn behandlingsansvarlig var klar over. Dette ble avdekket da Datatilsynet kom på kontroll. I dette tilfellet var det liten kunnskap om selve systemet som var problemet, men det er også mulig å se for seg at man ønsker å endre systemet. Enten for å rette opp feil, eller for å tilby en ny tjeneste<sup>265</sup>. Slike endringer kan bli svært kostbare om ikke programvaren er lagt opp på en slik måte at det enkelt lar seg endre. Manglende planlegging kan også føre til tungvinte løsninger som at man er nødt til å skaffe seg nytt (fysisk) kort dersom man ønsker å trekke tilbake et samtykke og fortsette å reise anonymt. I tilfellet Innlandskoret, ble påleggene fra Datatilsynet oppfattet som såpass tungvinte å rette seg etter, at de per dags dato har gått vekk fra registrerte kort.

Dette viser viktigheten av såkalt "privacy by design", altså systemene er laget for å være fleksible i forhold til lagring av opplysninger og å skille forskjellige typer data fra hverandre.

Å planlegge en god prosess eller skrive en god kravspesifikasjon forutsetter at man har oversikt over hvilke behov selskapet har og vil få, samt hvilke krav loven stiller.

### 7.3 Bransjenormen og veien videre

Datatilsynets kontroller av billettsystemer i 2009 og 2010 fant feil og svakheter hos samtlige aktører de kontrollerte. Trolig er det flere billettsystemer i Norge som ikke opererer i tråd med personopplysningslovens bestemmelser. Over har jeg pekt på

---

<sup>264</sup> I dette tilfellet kollektivselskapet.

<sup>265</sup> For eksempel å tilby muligheten til å registrere kortet sitt.

hva jeg tror kan være to av de viktigste årsakene til praksis som avviker fra lovens bestemmelser.

Samtidig er Bransjenormen en mulig løsning på disse to utfordringene. Normen tar stilling i de fleste av de juridiske avveiningene og vil også inneholde eksempler på god praksis dersom vedleggene godkjennes. Det viktigste her er bestemmelsene i normen sier noe konkret om hvordan man skal drifte et elektronisk billettsystem, ikke bare generelt om behandling av personopplysninger. Det er derfor vesentlig lettere å forholde seg til for ansatte uten spesiell juridisk kompetanse. Det er ikke nødvendigvis slik at det ikke vil dukke opp en del spørsmål mens Bransjenormen er ny, men da vil normen kunne oppdateres etter at spørsmålet er avklart. Trolig har arbeidet med utviklingen av Bransjenormen i større grad forberedt Datatilsynet på slike henvendelser også.

Datatilsynet ønsker å bruke Bransjenormen som utgangspunkt når de gjennomfører kontroller i fremtiden. Dermed vil ethvert kollektivselskap som setter seg inn i normen også vite hva de kan forvente ved en eventuell kontroll. Normen vil kunne gi kunnskap om hvilke spørsmål som må avklares i forkant av implementering av nye systemer og hvilke muligheter et slikt system må gi. Ettersom Bransjenormen er obligatorisk for en stor andel av kollektivselskapene i landet, er det grunn til å tro at den kan bli en standard som benyttes i bransjen. Om kravene i bransjen endrer seg vil det også kunne påvirke eksterne tilbydere av ferdige systemer som blir nødt å tilpasse seg kravspesifikasjonene i markedet.

Det forutsetter at Bransjenormen blir kjent og anvendt i bransjen, men trolig vil den kunne fungere som en pådriver i retning av en standardisering. En standardisering som på sikt vil gjøre det lettere for kollektivselskapene å følge lovens bestemmelse og styrke de reisendes personvern.

## Kilder:

### Litteratur:

Aftenposten, aften, 17.01.2012, s. 6: "Her er Oslos forvirrende kollektivkart".

Apenes, Georg og Hågen Ljøgodt (2009): *Høringsuttalelse - etterkontroll av personopplysningsloven*. Oslo: Datatilsynet.

Blekeli, Ragnar Dag og Knut S. Selmer (1977): *Data og personvern*. Oslo – Bergen – Tromsø: Fagbokforlaget.

Boe, Erik (2005): *Grunnleggende juridisk metode – En introduksjon til rett og rettstenkning*. Oslo: Universitetsforlaget.

*Bransjenorm - for personvern og informasjonssikkerhet i elektronisk billettering*, versjon 1.0, Oslo: Datatilsynet, 2011.

### Datatilsynets kontrollrapporter:

- *Endelig kontrollrapport 7. mai 2009*, Saksnr: 09/00163-15, 2009, Ruter AS.
- *Endelig kontrollrapport 21.03.2009*, Saksnr: 09/00195-9, 2010, Oppland Fylkeskommune.
- *Endelig kontrollrapport 02.04.2009*, Saksnr:09/00193-8, 2010, Kolumbus – Rogaland kollektivtrafikk.
- *Endelig kontrollrapport 25.10.2007*, Saksnr: 07/01381, 2007, Troms fylkeskommune.

Ellertsen, Kim og Jørgen Skorstad (2010): *Vedrørende stansing av saker til behandling i Personvernemnda*. Oslo: Datatilsynet, Brev fra Datatilsynet til Personvernemnda.

*Håndbok 206 Elektronisk billettering*, Statens Vegvesen - vegdirektoratet, 2011.

Lomell, Heidi Mork (2007), *Selektive overblikk: En studie av videoovervåkingspraksis*. Oslo: Universitetsforlaget.

Ottesen, Christine Ask og Katrine Berg Blixrud (2010): *Personvern i finanssektoren*, Oslo: Gyldendal Norsk Forlag.

*Personvernrapporten 2010*, Oslo: Datatilsynet, 2010.

Schartum, Dag Wiese (2008): *Norsk lovkommentar: personopplysningsloven*. Gyldendal Rettsdata.

Schartum, Dag Wiese og Lee A. Bygrave (2011): *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*. Bergen: Fagbokforlaget Vigmostad & Bjørke.

Stavanger Aftenblad, 01.10.2010 s. 4 " Fikk se samboerens bevegelser sort på hvitt".

## Rettskilder:

Et bedre personvern - forslag til lov om behandling av personopplysninger, Oslo: Statens forvaltningstjeneste, 1997. (NOU 1997:10).

European Union Directive on Data Protection Recitals, DIRECTIVE 95/46/EC I - on the protection of individuals with regard to the processing of personal data and on the free movement of such data, THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 24 October 1995. (Fortalen til EUs personverndirektiv).

*Forvaltningsloven. Lov om behandlingsmåten i forvaltningssaker* av 10. februar 1967.

*Individ og integritet - Personvern i det digitale samfunnet*, Oslo: Statens forvaltningstjeneste 2009. (NOU 2009:1).

*Offentlige persondatasystem og personvern*, Oslo: Statens forvaltningstjeneste, 1975. (NOU 1975:10).

*Opplæringslova. Lov om grunnskolen og den vidaregåande opplæringa* av 17. juli 1998 nr. 61.

*Ot.prp. nr. 92(1998-99) Om lov om behandling av personopplysninger (personopplysningsloven)*, Oslo: Justis- og politidepartementet, 1999.

*Personopplysningsforskriften. Forskrift om behandling av personopplysninger* av 15. desember 2000 nr. 1265.

*Personopplysningsloven. Lov om behandling av personopplysninger* av 14. april 2000 nr 31.

*Personregisterloven. Lov om personregistre m.m.* av 9. juni 1978 nr. 48 (Opphevet).

*Personverndirektivet. EUROPAPARLAMENTS- OG RÅDSDIREKTIV 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger* av 24. oktober 1995.

## Personvernemndas klagesaker:

- PVN-2005-11, Klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner, Personvernemndas avgjørelse av 7.3.2006.
- KLAGESAK 2004/01: Klage på Datatilsynets vedtak om vilkår om samtykke for konsesjon for delstudie 1 og 2 – Statens Arbeidsmiljøinstitutt – STAMI, Personvernemndas avgjørelse av 19.08.04.
- KLAGESAK 2003/01: Klage på Datatilsynets vedtak i sak om avslag på konsesjonssøknad for opprettelse av sentralt låneregister.
- KLAGESAK 2005-06: Klage på vedtak om pålegg i forbindelse med tilsyn hos Securitas, samt begjæring om at deler av vedtaket gis oppsettende virkning, Personvernemndas avgjørelse av 06.12.2005.

- PVN-2006-06: Dopingprøver. Klage på Datatilsynets vedtak om at dopingtester ved treningssenteret Skullerud Sport Senter AS skal opphøre, Personvernemndas avgjørelse av 14. september 2006.

### Internettkilder:

*Befolkningsendringer 2010 - 2011*: Statistisk sentralbyrå , 2011,

URL:<http://www.ssb.no/folkendrkv/arkiv/tab-2011-02-24-02.html> [lesedato: 20.08.2012].

Buskerud kollektivtransport AS, "*Velkommen som busspilot på linje 169*", URL:

<http://www.bk.no/Billetterogreisekort/Nyttbillettsystem169.aspx> [lesedato: 01.02.2012].

Datatilsynet, *Alfabetisk oversikt over personvernombudene*, 20.12.2011,

<http://www.datatilsynet.no/Personvernombud/Alfabetisk-oversikt-over-personvernombud/> [lesedato: 15.08.2012].

Datatilsynets meldingsdatabase, *meldingssøk*, URL:

[http://hetti.datatilsynet.no/melding/report\\_search.pl](http://hetti.datatilsynet.no/melding/report_search.pl) [lesedato: 20.08.2012].

Fornyings- og administrasjonsdepartementet, *Hva er personvern?*, URL:

<http://www.regjeringen.no/nb/dep/fad/tema/personvern/hva-er-personvern.html?id=448290> [lesedato:01.02.2012].

Hansen Anette Holth, Olav Juven, Knut Erik Solhaug (2012), "*Kan bli rushtidsavgift på all kollektivtrafikk i Oslo-området*" I: NRK Østlandssendingen, Nettutgaven,

18.04.2012, URL: <http://nrk.no/nyheter/distrikt/ostlandssendingen/1.8079403>

[lesedato: 18.05.2012].

### Innlandskortets hjemmesider:

- Innlandskortets hjemmesider, *Forside*, URL: <http://www.innlandskortet.no/> [lesedato: 20.05.2012]
- Innlandskortets hjemmesider, *Registrering*, URL: <http://www.innlandskortet.no/registrere/> [lesedato: 02.04.2012].
- Innlandskortet shjemmesider, *Nyttig å vite*, URL: <http://www.innlandskortet.no/statisk/16/> [lesedato: 02.07.2012].
- Innlandskortets hjemmesider, *Ofte stilte spørsmål*, URL: <http://www.innlandskortet.no/statisk/14/> [lesedato: 02.07.2012].
- Innlandskortets hjemmesider, *Personvern*, URL: <http://www.innlandskortet.no/personvern/> [lesedato: 02.07.2012].
- Innlandskortets hjemmesider, *PDF om personvern*, URL: <http://www.innlandskortet.no/filer/lastned/3/0/> [lesedato: 16.06.2012]

Kervarec, Varog og Kurt Lekanger (2012), "*Så mye er lagret om deg*" I: Mobilen.no,

04.06.2012, URL: <http://www.mobilen.no/artikler/sa-mye-er-lagret-om-deg/109793> [lesedato: 07.06.2012].

Oslotrikken, *Årsrapport Oslo Sporvognsdrift AS 2006*, 08.03.2007, URL: [http://www.trikken.no/OpplastedeBilder/DivBilde/OSSP0026\\_Aarsrapport.pdf](http://www.trikken.no/OpplastedeBilder/DivBilde/OSSP0026_Aarsrapport.pdf) [lesedato: 20.08.2012].

### Ruters hjemmesider:

- Ruters hjemmesider, *Kupongkort*, 30.08.2011, URL: [http://ruter.no/no/billetter/oslo\\_og\\_akershus/kupongkort/](http://ruter.no/no/billetter/oslo_og_akershus/kupongkort/) [lesedato: 20.08.2012].
- Ruters hjemmesider, *MinSide*, URL: <http://ruter.no/no/billetter/reisekortet/MinSide/> [lesedato: 02.07.2012].
- Ruters hjemmesider, *Personvern*, URL: <http://www.ruter.no/personvern> [lesedato: 02.07.2012].
- Ruters hjemmesider, *Behandling av personopplysninger*, URL: [http://ruter.no/no/verdt-a-vite/Om-Ruter/personvern/personvern\\_reisekort/](http://ruter.no/no/verdt-a-vite/Om-Ruter/personvern/personvern_reisekort/) [lesedato: 14.06.2012].
- Ruters hjemmesider, *Om Reisekortet*, URL: <http://ruter.no/no/billetter/reisekortet/> [lesedato: 02.07.2012].

Skoleskyss.no, *Om Skoleskyss*, URL: <http://www.skoleskyss.no/index.php/om-skoleskyss> [lesedato: 20.08.2012].

Sør-Trøndelag Fylkeskommune, *Fylkesrevisjonen*, 30.04.2003, URL: <http://www.revisjonmidtnorge.no/rapporter/2003-elektroniskbillettering.pdf> [lesedato: 20.08.2012].

Wikipedia, *Flexus*, URL: <http://no.wikipedia.org/wiki/Flexus> [lesedato: 20.05.2012].

Zachariassen, Espen (2010), " *Flexus: – En syretest på personkartlegging*" I: Teknisk Ukeblad, 07.05.2010, URL: <http://www.tu.no/it/2010/05/07/flexus--en-syretest-pa-personkartlegging> [lesedato: 02.05.2011].